UNITED ARAB EMIRATES
MINISTRY OF JUSTICE

Guidebook

for Law Firms and Legal Consultancy Offices on Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF)

UNITED ARAB EMIRATES
MINISTRY OF JUSTICE

Guidebook

for Law Firms and Legal Consultancy Offices on Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF)

Drafted by

Judge/ Dr. Abdullah Ahmad Jasem Al-Rashed

Director of the Anti-Money Laundering and Counter-Terrorism Financing Department

Ministry of Justice

Second Edition

1447 A.H. – 2026 A.D.

Second Edition
1447 AH - 2026 AD
United Arab Emirates

Publication Title : Guidebook for Law Firms and Legal Consultancy Offices on Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF)

Publication Type: Booklet (Guide Book)

Language : English

Publisher : Ministry of Justice

INDEX

Objectives of this guidebook

The Ministry of Justice, through the issuance and publication this guidebook, aims to inform the Designated Non-Financial Businesses and Professions (DNFBPs) - specifically law firms and legal consultancy offices - of the following:

1. Ensuring compliance with Federal Decree-Law No. (10) of 2025 Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF), its Executive Regulations issued by Cabinet Resolution No. (134) of 2025, and the implementing decisions.
2. Outlining the key duties and obligations in accordance with Federal Decree-Law No. (10) of 2025 Concerning Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF), its Executive Regulations, and the implementing decisions.
3. Clarifying methods for identifying, assessing and mitigating the risks of money laundering and terrorist financing.
4. Outlining the reporting procedures and mechanism for reporting suspicious transactions or suspicious activities.
5. Enhancing protection against the exploitation of their firms and establishments in money laundering and terrorist financing crimes, while safeguarding the reputation and integrity of the profession.
6. Strengthening institutional compliance within law firms by encouraging the adoption of effective internal policies and procedures, appointing a Compliance Officer, and providing continuous staff training.
7. Reinforcing and protecting the credibility and integrity of the country's financial system.

This guidebook, along with the instructions and guidelines it contains, does not lead to the creation of additional new legal obligations, but have been prepared for the purpose of explanation and clarification of the obligations and requirements stipulated in Federal Decree-Law No. (10) of 2025 Concerning Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF), its Executive Regulations, and the implementing decisions. The content of this guidebook is provided for illustrative and explanatory purposes only, and shall not be construed as exhaustive or restrictive. Accordingly, this guidebook does not substitute for reference to Federal Decree-Law No. (10) of 2025 Concerning Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF), its Executive Regulations, or any decisions issued in implementation thereof."

The Concept of Money Laundering

A significant number of criminal acts are committed with the primary objective of generating profit for the individual or group perpetrating the offense. Money laundering constitutes a process through which these illicit proceeds are handled with the intent to conceal their unlawful origin. When a criminal activity yields substantial financial gains, the principal concern of those involved becomes finding a method to control and utilize the funds without drawing attention to the underlying illegal activity. To achieve this, perpetrators typically obscure the sources, alter the form, or transfer the funds to locations where they are less likely to attract attention.

Under UAE law, money laundering is defined as any financial or banking transaction intended to conceal or alter the identity of funds obtained through illegal means, by channelling them through the financial and banking system in a manner that makes them appear to originate from legitimate sources. These funds are then reinvested or reintroduced into the economy in a legally structured form that contradicts their true nature.

Money laundering refers to the commission or attempted commission of any act intended to conceal or disguise the origin or reality of funds acquired in violation of Sharia or statutory law, making them appear as if they are lawfully sourced.

Article (2) of Federal Decree-Law No. (10) of 2025 Concerning Anti-Money Laundering stipulates:

1. A person shall be deemed to have committed the crime of money laundering if he knows, or if there are sufficient indications or presumptions of his knowledge, that all or part of the funds are proceeds of a predicate offence, and he intentionally undertakes any of the following acts:
    A. Converts, transfers, or carries out any transaction involving the proceeds, with the intent to conceal or disguise their illicit source.
    B. Conceals or disguises the true nature of the proceeds, their source, location, manner of disposition, movement, ownership, or the rights pertaining thereto.
    C. Acquires, possesses, or uses the proceeds upon receipt thereof.
    D. Assists the perpetrator of the predicate offence in evading punishment.

2. The crime of money laundering shall be considered an independent offence, exempt from the application of the rules of concurrence provided for in Federal Decree-Law No. (31) of 2021 referred to herein, and the punishment or non-punishment of the perpetrator of the predicate offence shall not preclude his punishment for the crime of money laundering.
3. A conviction for the predicate offence shall not be required to establish the illicit source of the proceeds, nor shall knowledge of the type or precise nature of the predicate offence be required. Knowledge, as an element of the crime, may be inferred from the factual and objective circumstances of its commission.

Predicate Offense

Federal Decree-Law No. (10) of 2025 defines the Predicate Offense as any act that constitutes a felony or misdemeanor, including offences of terrorism financing, financing the proliferation of weapons, and evasion of direct or indirect taxes, in accordance with the applicable legislation in the Country, whether committed within or outside the Country, provided that it is punishable in both jurisdictions.

The implication of this definition is that a predicate offense refers to any offense — whether a felony or misdemeanor — that is punishable under the laws of the United Arab Emirates, regardless of whether it is committed within the UAE or in another country, as long as the act is criminalized and punishable in both the UAE and the foreign jurisdiction where the act occurred.

Stages of the Money Laundering Process

The process of money laundering typically consists of three fundamental stages:

1. Placement Stage
2. Layering Stage
3. Integration Stage

A simplified explanation of each stage is provided below:

1. Placement Stage:

This stage involves the initial introduction or substitution of illicit funds - often fragmented into smaller amounts - into legitimate investment projects. The money launderer deposits the illegal proceeds into the formal channels of the financial and banking system in a manner that avoids detection. This stage may be executed through various methods, including: depositing funds into banks or financial institutions, converting the funds into foreign currencies, dividing the funds into small amounts and depositing them into banks, repaying legitimate loans using laundered money, or physically transporting cash across borders

2. Layering Stage

The objective of this stage is to obscure the illicit origin of the deposited funds and to eliminate suspicion regarding their unlawful source, thereby making them difficult to trace. This may be achieved through: conducting transfers between multiple accounts, linking funds through a network of accounts across different global locations, moving funds between financial institutions or within multiple accounts in the same institution, investing in stocks, bonds, or life insurance products, exchanging funds for traveler's checks or bank drafts, or investing in real estate or other legitimate ventures, and using shell companies to conceal the identity of the ultimate beneficial owner and the assets

3. Integration Stage

The goal of this stage is to re-inject the laundered funds into the economy and to legitimize them by integrating them into the national or international financial system. This is typically done through: direct investments in real estate, acquiring rare goods such as antiques and valuable items, purchasing shares in companies, or investing in the stock market, and so on.

Countering Proliferation Financing (CPF) in line with international standards and national legislation

Financing of the Proliferation of Weapons:

This term refers to the risk of collecting, moving, or generating funds, other assets, and other economic resources, or the full or partial financing of individuals or entities for the purposes of the proliferation of weapons of mass destruction (WMD), including the proliferation of their delivery systems or related materials, such as dual-use technology and dual-use goods exploited for unlawful purposes.

The UAE legislator has defined the financing of weapons proliferation as the unlawful and unauthorized dealing - as regulated under the legislation in force in the State - in materials, systems, equipment, components, programs, or technology that contribute to the production or development of weapons of mass destruction, the related technology, or their means of delivery. This also includes any act specified under Clause (3) of Article (3) of Federal Decree-Law No. (10) of 2025.

Stages of Financing the Proliferation of Weapons:

1. The Stage of Raising Funds for Weapons Proliferation Programs:

A country that maintains a weapons program collects the financial resources needed to cover domestic program costs. Sources of funding may include the national budget allocated to such programs, while profits may originate from a network of overseas commercial companies and proceeds generated from criminal activities conducted abroad.
(Example: mechanisms used to raise funds for a weapons proliferation program.)

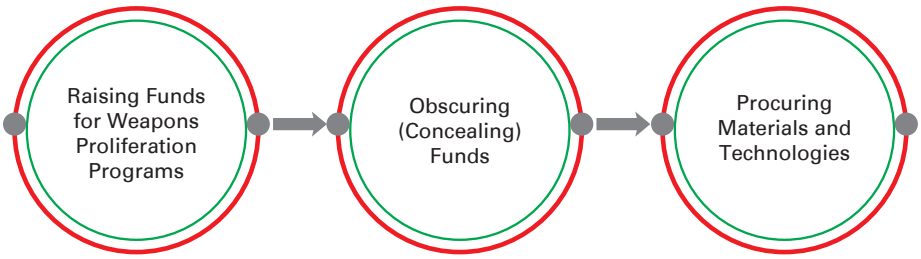
2.The Stage of Obscuring (Concealing) Funds:

A state with weapons programs transfers assets into the international financial system, often involving foreigncurrency exchange transactions for traderelated purposes. A country pursuing a weapons program may resort to a range of methods - from simple techniques to highly complex schemes - using normal correspondent banking channels or a sophisticated network of procurement agents and front companies. At this stage, countries subject to comprehensive sanctions attempt to circumvent such sanctions by employing often advanced methods to disguise the movement of funds.

3. The Stage of Procuring Materials and Technologies:

The country with weapons programs, or its agents, uses concealed resources to procure materials and technologies through the international financial system. This stage includes making payments for the shipment and transfer of such materials and technologies

Stages of Financing the Proliferation of Weapons:



Dual-Use Goods:

Dual-use goods are items that have both civilian and military applications. These goods are often subject to government control through export-control regulations, which may restrict the export of certain items depending on the end-user and the end-use, unless prior governmental authorization is obtained.

Law firms and legal consultancies must recognize that dual-use goods are frequently subject to export-control requirements. They should seek to identify such goods in transactions, apply enhanced due diligence to these operations, and review the list of controlled goods and materials (Cabinet Decision No. 50 of 2020). The import and export of dual-use goods require authorization from the relevant competent authorities.

Trade-finance documents for shipments and letters of credit typically do not contain the level of detail necessary to determine whether the goods are subject to export controls. However, private-sector institutions may still be able to detect certain export-related red flags within transactions. Where there is a reasonable level of suspicion that the goods involved may be used in the development, production, or use of materials related to weapons of mass destruction, the client must be asked to provide additional information about the goods, including their technical specifications, end-use, and end-user.

Preventive Measures to Mitigate and Reduce Proliferation-Financing Risks:

Law firms and legal consultancies must take appropriate steps to manage and mitigate proliferation-financing risks when such risks are identified in the firm's institutional risk assessment.

Firms are required to ensure that their internal policies and procedures adequately address proliferation and proliferation-financing risks, in line with national guidance, the directives issued by the Executive Office for Control and Non-Proliferation, the relevant supervisory authorities, and the international standards issued by the Financial Action Task Force (FATF), in a manner that ensures the effectiveness of internal controls in reducing related risks.

Key preventive measures and mitigation procedures may include the following:

1. Periodically updating internal policies and procedures to align with legislative developments and international regulatory requirements related to proliferation financing.
2. Enhancing Customer Due Diligence (CDD) measures and ensuring verification of the client's identity and the beneficial owner, as well as collecting sufficient information regarding the nature of the client's activities and the sources of their funds.
3. Applying Enhanced Due Diligence (EDD) to high-risk clients, particularly in cross-border transactions or those involving dual-use materials or goods.
4. Conducting periodic screening against targeted financial sanctions lists, both international and domestic.
5. Verifying all parties involved in a transaction, including intermediaries, suppliers, and shipping companies, and ensuring they are not linked to sanctions lists or high-risk activities.
6. Reporting suspicious transactions where there is reasonable suspicion of a connection to proliferation financing or attempts to circumvent controls.
7. Documenting all procedures and retaining client and transaction records for five years from the date of completion of the work, to facilitate inspection or audit processes.
8. Providing continuous staff training on proliferation-financing red flags and methods for detecting transactions involving dual-use goods.

Guidance Manual on Countering Proliferation Financing (CPF):

The Executive Office for Control and Non-Proliferation (EOCN) has prepared a guidance manual on countering the financing of weapons proliferation, targeting financial institutions, designated non-financial businesses and professions (DNFBPs), and virtual asset service providers (VASPs).

The purpose of this manual is to raise awareness of the threats, risks, and vulnerabilities associated with the financing of weapons proliferation, and to support the identification, assessment, and mitigation of proliferation risks in accordance with the standards of the Financial Action Task Force (FATF).

The Anti-Money Laundering Department recommends reviewing this manual to obtain a more comprehensive, in-depth, and detailed understanding of all matters related to the financing of weapons proliferation.

The manual is available on the official website of the Executive Office for Control and Non-Proliferation, as well as on the Ministry of Justice website under Laws and Legislation - Anti-Money Laundering and Counter-Terrorism Financing - Guidance Materials

Designated Non-Financial Businesses and Professions (DNFBPs)

Federal Decree-Law No. (10) of 2025 on Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) defines Designated Non-Financial Businesses and Professions (DNFBPs) as: "Any person engaged in one or more commercial or professional activities as specified in the Executive Regulations of this Decree-Law".

Referring to the Executive Regulations issued under Cabinet Decision No. (134) of 2025, Clause (4) of Article (3) states that the following are considered DNFBPs:

Lawyers, notaries, other independent legal professionals, and independent accountants, when they prepare, execute, or carry out financial transactions on behalf of their clients in relation to the following activities:

A. Purchase and sale of real estate
B. Management of client-owned funds
C. Management of bank accounts, savings accounts, or securities accounts
D. Organization of contributions for the establishment, operation, or management of companies
E. Establishment, operation, or management of legal persons or legal arrangements
F. Purchase and sale of business entities

Relevant Legislation

1. Federal Decree-Law No. (10) of 2025 on Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF).
2. Cabinet Decision No. (134) of 2025 issuing the Executive Regulations of Federal Decree-Law No. (10) of 2025 on Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF).
3. Cabinet Decision No. (3/1 W) of 2019 designating the Ministry of Justice as the supervisory authority over lawyers and notaries in the UAE.
4. Cabinet Decision No. (74) of 2020 concerning the Terrorist List System and the implementation of UN Security Council resolutions on the prevention and suppression of terrorism and its financing, and the prevention of proliferation and its financing, and related decisions.
5. Cabinet Decision No. (71) of 2024 regulating administrative violations and penalties applicable to entities subject to Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) supervision by the Ministry of Justice and the Ministry of Economy.
6. Minister of Justice Decision No. (248) of 2025 regulating procedures and supervisory controls over law firms, legal consultancies, and notaries in the field of Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT).

Supervisory Authority over Lawyers

Cabinet Decision No. (1/3 W) of 2019 established the institutional framework for supervising Designated Non-Financial Businesses and Professions (DNFBPs) within the UAE. Under this decision, the Ministry of Justice was designated as the supervisory authority over lawyers and notaries in the country.

Subsequently, Minister of Justice Decision No. (532) of 2019 was issued concerning the establishment of the Anti-Money Laundering and Counter-Terrorism Financing Section. Article (4) of this decision stipulates that the newly established section within the Ministry of Justice shall be responsible for supervising, monitoring, and overseeing Designated Non-Financial Businesses and Professions (DNFBPs) across the UAE, including entities operating in free zones and financial free zones, in accordance with the Ministry's obligations under the Decree-Law and its Executive Regulations.

Over time, and in light of the section's notable achievements and its demonstrated effectiveness in fulfilling its assigned duties, and in response to organizational needs and the commitment to institutional empowerment, Cabinet Decision No. (65) of 2024 was issued concerning the organizational structure of the Ministry of Justice. This decision upgraded the section to a full-fledged department under the Judicial Services Sector of the Ministry of Justice, thereby reinforcing its role as a core component of the national framework for combating money laundering and terrorism financing.

Anti-Money Laundering and Counter-Terrorism Financing Department

Cabinet Decision No. (65) of 2024 concerning the organizational structure of the Ministry of Justice outlines the duties and responsibilities of the Department for Anti-Money Laundering and Counter-Terrorism Financing as follows:

1. Identifying and assessing risks related to the Designated Non-Financial Businesses and Professions (DNFBPs) under the Ministry's supervision.
2. Establishing and continuously updating an integrated database of Designated Non-Financial Businesses and Professions (DNFBPs) subject to the Ministry's oversight.
3. Receiving and responding to inquiries from Designated Non-Financial Businesses and Professions (DNFBPs) regarding procedures and regulatory systems.
4. Implementing and monitoring the Ministry's operational plan for combating money laundering and terrorism financing.
5. Conducting desk-based and field inspections of Designated Non-Financial Businesses and Professions (DNFBPs) under the Ministry's supervision based on:
   A. The national risk assessment.
   B. Crime-related risks, internal policies, controls, and procedures applicable to the supervised sector, as defined in the approved risk assessment.
6. Maintaining an up-to-date list of compliance officers within Designated Non-Financial Businesses and Professions (DNFBPs) under the Ministry's supervision and notifying the Financial Intelligence Unit accordingly.
7. Issuing guidelines, instructions, and templates related to anti-money laundering and countering the financing of terrorism for DNFBPs under the Ministry's supervision, as needed.
8. Organizing awareness programs and campaigns for Designated Non-Financial Businesses and Professions (DNFBPs) and their staff on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) obligations.
9. Verifying Designated Non-Financial Businesses and Professions' (DNFBPs) compliance with the obligations set forth in Federal Decree-Law No. (10) of 2025 on Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF), its Executive Regulations, and related implementing decisions.

10. Taking all necessary measures to ensure Designated Non-Financial Businesses and Professions (DNFBPs) comply with UN Security Council resolutions on the prevention and suppression of terrorism and its financing, and the prevention and suppression of the proliferation of weapons of mass destruction and their financing, including field visits, ongoing monitoring, and the imposition of appropriate administrative penalties in case of violations or non-compliance.
11. Reporting to the Executive Office for Control and Non-Proliferation (EOCN) any notifications, information, or data received from Designated Non-Financial Businesses and Professions (DNFBPs) regarding listed individuals or entities.
12. Preparing reports on violations committed by Designated Non-Financial Businesses and Professions (DNFBPs)under the Ministry's supervision.
13. Notifying Designated Non-Financial Businesses and Professions (DNFBPs) of administrative sanctions issued against them.
14. Preparing periodic statistics on measures taken, corrective actions implemented, and penalties imposed on Designated Non-Financial Businesses and Professions (DNFBPs) under the Ministry's supervision.
15. Performing any other functions related to the nature of the Department's work, in accordance with applicable legislation or as assigned by the Minister.

In implementation of the above-mentioned Cabinet Decision No. (65) of 2024, Minister of Justice Decision No. (248) of 2025 was issued to regulate the procedures and supervisory controls over law firms, legal consultancies, and notaries in the field of anti-money laundering and Countering the Financing of Terrorism.

International Organizations

Numerous international organizations are actively engaged in combating money laundering, terrorism financing, and the proliferation of weapons of mass destruction. The most prominent among these include:

1. The Financial Action Task Force (FATF)
2. The International Monetary Fund (IMF)
3. The International Organization of Securities Commissions (IOSCO)
4. The International Criminal Police Organization (INTERPOL)
5. The Middle East and North Africa Financial Action Task Force (MENAFATF)
6. The Inclusive Framework on Base Erosion and Profit Shifting (BEPS) under the G20 and the Organisation for Economic Co-operation and Development (OECD)
7. The United Nations (UN)

The United Arab Emirates is a member or party to many of these organizations. Their requirements and recommendations are integrated into the core components of the national framework for anti-money laundering and Countering the Financing of Terrorism.

Obligations and Duties of Legal Professionals

Designated Non-Financial Businesses and Professions (DNFBPs), law firms and legal consultancy offices, are required to comply with all provisions set forth in Federal Decree-Law No. (10) of 2025, its Executive Regulations, and the implementing decisions issued thereunder. Key obligations include:

1. Identifying, assessing, and understanding the risks associated with money laundering and terrorism financing.
2. Establishing appropriate policies and internal controls to mitigate and manage such risks.
3. Implementing customer due diligence procedures.
4. Appointing a Compliance Officer.
5. Reporting suspicious transactions to the relevant authorities.
6. Complying with requirements related to emerging technologies.
7. Maintaining adequate records and documentation.
8. Conducting training programs and awareness initiatives.
9. Enforcing targeted financial sanctions.
10. Preventing the financing of weapons proliferation.

Identification, Assessment, and Understanding of Money Laundering and Terrorism Financing Risks

Lawyers are required to identify and assess the risks of money laundering and terrorism financing within their practice, and to document such assessments in writing. These risk assessments and the associated information must be updated periodically.

Law firms must also be prepared to submit their risk assessment reports and related documentation to the regulatory authorities - namely, the Ministry of Justice - upon request. The nature of the risk assessment process must be proportionate to the size and scope of the law firm's operations.

Conducting a risk assessment enables law firms and legal consultancy offices to allocate resources more efficiently and effectively, identify gaps and opportunities for improvement in their Anti-Money Laundering, Countering the Financing of Terrorism (AML/CFT) policies, procedures, and internal controls, and make informed administrative decisions regarding their risk appetite. It also supports the adoption and implementation of appropriate risk mitigation measures and strategies.

The risk assessment process involves identifying the inherent risks faced by the law firm, institution, or individual lawyer, and determining how these risks can be effectively mitigated through the firm's established policies, procedures, and internal controls.

It is important to note that prior to conducting a risk assessment, lawyers must understand that money laundering and terrorism financing risks may be classified as either high or low.
If the identified risks are high, enhanced measures must be applied that are proportionate to the level of risk in order to mitigate it. Conversely, if the risks are low, the firm or institution may adopt simplified measures to manage and reduce the risk. However, it is imperative to note that lawyers, legal consultants, or compliance officers are strictly prohibited from applying simplified measures in cases where there is any suspicion of money laundering.

Risk Identification and Assessment

The first step in conducting a risk assessment related to Anti-Money Laundering, Countering the Financing of Terrorism (AML/CFT) for lawyers is to identify, assess, and understand the inherent risks of money laundering and terrorism financing across all activities. This process should focus on the following risk factors:

1. Client-related risk factors
2. Geographic risk factors, including the countries or regions where clients operate, the origin of the transaction, or its final destination
3. Risks arising from the nature of the products, services, or transactions, and the channels through which they are delivered

When assessing inherent risks, lawyers should compile a list of clients, identify the products and services provided to those clients, and determine the countries and regions in which the clients conduct business. Risks often emerge as a combination of these factors.

Lawyers may develop risk scenarios based on these factors and evaluate the likelihood of their occurrence, as well as the potential impact if such scenarios materialize. Likelihood may be assessed based on the frequency with which such risks could occur annually, while impact may be evaluated in terms of financial consequences and reputational damage that could result from the realization of the scenario.

Through this approach, lawyers can identify the inherent risks associated with each risk factor. Based on the identified inherent risks, they can then assess the effectiveness of existing risk mitigation measures and determine whether any residual risks remain. If residual risks are identified that fall outside the scope of previously assessed risks, additional controls must be implemented.

Client Risks

Client risk factors pertain to the types or categories of clients to whom legal services are provided. Certain categories of clients or business relationships may present risks that must be considered when assessing the overall level of inherent client risk.

When identifying specific client categories as inherently high-risk, lawyers must take into account the findings of sectoral or thematic risk assessments, as well as information from official sources, including the National Risk Assessment, the Financial Action Task Force

(FATF), and the Middle East and North Africa Financial Action Task Force (MENAFATF). Examples of high-risk scenarios include:

1. Business relationships conducted under unusual circumstances
2. Clients who are non-residents of the country
3. Legal persons or arrangements used as instruments for asset holding
4. Companies with nominee shareholders or bearer shares

Risks Arising from the Nature of Products, Services, or Processes and Delivery Channels

When assessing the inherent risks of money laundering and terrorist financing associated with legal services, lawyers must evaluate which of their services are most vulnerable to misuse. This includes assessing the inherent risks posed by clients who may exploit services for illicit purposes, taking into account factors such as the ease of retaining and transferring value, complexity, and transparency.

Risks Arising from Geographic Locations and Delivery Channels

Law firms and legal consultancy offices may be exposed to geographic risks of money laundering and terrorist financing from both domestic and cross-border sources. These risks may arise from:

1. Locations where the lawyer or law firm maintains offices or branches
2. Locations where clients reside or conduct their activities

With respect to geographic risks, lawyers and legal consultants may obtain information from the National Committee for Combating Money Laundering to identify high-risk countries and those under enhanced monitoring.

When evaluating risks related to delivery channels, lawyers should pay particular attention to channels that obscure or attempt to obscure client identity. These may include, for example, indirect communication channels (non-face-to-face), remote service delivery without in-person interaction - especially where safeguards such as electronic identity verification are absent - such as internet or telephone services, other remote communication technologies, the use of complex legal entities, intermediaries, agents, or third-party distributors, unexplained cash payments, or receipt of funds from third parties without clear justification.

These channels pose a heightened risk of exploitation for money laundering or terrorist financing. Accordingly, enhanced due diligence procedures must be applied, and the rationale for using such channels must be documented within the internal policy framework of the law firm or legal consultancy.

Emerging Technologies

Attorneys, legal consultancy firms, and notaries are required to keep pace with modern technological developments related to money laundering and terrorist financing. This is particularly critical when assessing risks associated with the development of new legal products or the adoption of innovative professional practices, including new service delivery methods, technologies, or products offered in unconventional formats.

Such developments may include, for example, the use of digital currencies, rapid transfer applications, crowdfunding platforms, and artificial intelligence technologies used to conceal the origins of funds.

Accordingly, appropriate preventive measures must be taken prior to the launch or use of any such tools or practices. This includes conducting a thorough risk assessment and implementing effective controls to manage and mitigate those risks, in alignment with compliance obligations and professional oversight requirements.

Risk Mitigation

Law firms and legal consultancy offices are obligated to work toward reducing identified risks, taking into account any risks determined at the national level and the outcomes of their assessments. This shall be achieved through the following:

1. Establishing internal policies, controls, and procedures proportionate to the nature and scale of their operations, approved by senior management, enabling the firm to manage identified risks, monitor implementation, and enhance measures as necessary.
2. Implementing enhanced due diligence measures to manage high-risk scenarios upon identification, which may include, for example:

A. Obtaining and verifying additional information, such as client identity, beneficial ownership, the purpose of the business relationship, or the rationale behind a transaction.
B. Updating client and beneficial owner due diligence information more frequently.
C. Taking reasonable steps to determine the source of funds of the client and the beneficial owner.
D. Increasing the level and intensity of ongoing monitoring of the business relationship and scrutinizing transactions to identify any unusual or suspicious activity.
E. Obtaining senior management approval prior to establishing a business relationship with a client.

Following the completion of a risk assessment and based on its findings, law firms must develop and implement internal policies, procedures, and controls to combat money laundering and terrorist financing. These measures must define the appropriate level and type of intervention required to effectively manage and mitigate such risks. Firms must also monitor the implementation of these policies and procedures and reinforce them whenever necessary.

Establishment of Internal Policies, Procedures, and Controls

Pursuant to the provisions of the law and its executive regulations, law firms and legal consultancy offices are required to establish internal policies, procedures, and controls aimed at combating criminal activity. These measures must be aligned with relevant legislation and tailored to the risks, nature, scale, and complexity of the operations they may encounter. They must also be updated on an ongoing basis.

Such policies and procedures must be applied across all majority-owned branches and disseminated to all employees. Specifically, these internal measures shall include:

1. Customer due diligence measures and risk management procedures for business relationships.
2. Procedures for reporting suspicious transactions.
3. Appropriate compliance management arrangements to combat criminal activity, including the appointment of a Compliance Officer and a clear statement of their responsibilities.
4. Screening procedures to ensure high standards of competence and suitability in employee recruitment.
5. Development of regular training programs and workshops in the field of anti-money laundering and counter-terrorism financing to build the capacity and qualifications of compliance staff and other relevant personnel.

Definition of Due Diligence Measures

Federal Decree-Law No. (10) of 2025 and its executive regulations define due diligence measures as the process of identifying and verifying the information of a customer and beneficial owner - whether a natural person, a legal Person, or a legal arrangement -including the nature of their business, the purpose of the business relationship, and the ownership and control structure, including continuous monitoring procedures for the purposes of this Federal Decree-Law and its Implementing Regulation.

Lawyers are required to undertake due diligence measures with respect to clients prior to establishing a business relationship, continuing such a relationship, or executing a transaction. If such measures cannot be undertaken, the lawyer is prohibited from initiating or continuing the relationship or executing the transaction, and must report the matter to the Financial Intelligence Unit via a suspicious transaction report (STR).

The identification and assessment of money laundering risks, along with the implementation of reasonable and appropriate due diligence procedures and ongoing monitoring of client relationships, constitute a fundamental and effective component in combating money laundering and terrorism financing.

In certain cases, a lawyer may be unable to access information or conduct precise monitoring of client activities and transactions on an ongoing basis. In such instances, it is essential to focus on the effectiveness of the due diligence procedures undertaken.

Customer Due Diligence Measures

Lawyers and legal consultants shall undertake customer due diligence (CDD) measures in the following circumstances:

1. When initiating a business relationship.
2. When conducting occasional transactions for a client amounting to or exceeding AED 55,000, whether as a single transaction or multiple transactions that appear to be linked.
3. When conducting occasional transactions in the form of wire transfers amounting to or exceeding AED 3,500.
4. Where there is suspicion of criminal activity.
5. Where there are doubts regarding the accuracy or sufficiency of previously obtained customer identification data.

Lawyers and legal consultants are prohibited from engaging in the following activities:

1. Dealing with shell banks in any form, including opening bank accounts for them or accepting funds or deposits from them.
2. Opening or maintaining bank accounts under pseudonymous, fictitious, or anonymous names, or accounts identified only by numbers without the names of their holders.

Due diligence measures are procedures that lawyers must observe prior to establishing a business relationship, opening an account, or executing a transaction for a client with whom no prior relationship exists. These measures include, but are not limited to:

1. Verifying the official identification of the client and the beneficial owner, whether permanent or occasional, whether a natural person, legal person, or legal arrangement, and ensuring that any third party claiming to act on behalf of the client is properly authorized to do so.
2. Clearly understanding the nature and intended purpose of the business relationship with the client, ensuring it is reasonable and supported by reliable information, and obtaining relevant details as needed.
3. Understanding the nature of the client's business, ownership structure, and control mechanisms.
4. Applying enhanced due diligence measures to high-risk clients.
5. Verifying the legal status of all clients who ultimately own or control the entity, or who conduct transactions on their behalf, prior to commencing engagement.

Verification of the Identity of the Client and the Beneficial Owner – Natural Persons

Verification of the official identification of clients and beneficial owners who are natural persons shall be conducted using documents, data, or information obtained from a reliable and independent source, including:

1. Full name as stated in a valid identity card or travel document, with a certified copy of the valid document attached.
2. Nationality.
3. Address and place of birth.
4. Name and address of employer.
5. Obtaining senior management approval if the client or beneficial owner is a politically exposed person (PEP).

Verification of Identity of the Client – Legal Persons and Legal Arrangements

Verification of the official identification of clients who are legal persons or legal arrangements shall be conducted using documents, data, or information obtained from a reliable and independent source, including:

1. Name, legal form, and articles of incorporation.
2. Address of the registered office or principal place of business. If the entity is foreign, the name and address of its legal representative in the UAE must be provided, along with supporting documentation.
3. Memorandum of association or equivalent documents approved by the competent authority in the UAE.
4. Names of relevant individuals holding senior management positions within the legal person or legal arrangement.

Verification of Beneficial Owners – Legal Persons and Legal Arrangements

Verification of the identity of beneficial owners of legal persons and legal arrangements shall be conducted using reliable information, data, or documentation as follows:

1. Clients who are legal persons:
    A. Obtaining official identification of the natural person, whether acting alone or jointly with another, who holds a controlling ownership interest of 25% or more in the legal entity. If such identification cannot be obtained, or if there are doubts regarding the accuracy of the information provided, the identity shall be verified through alternative reliable means.
    B. If the controlling natural person cannot be identified under (a), or if the controlling shareholder is not the beneficial owner, then the identity of the natural person(s) holding senior management positions shall be determined.
2. Clients who are legal arrangements:
    A. Identifying the trustee, settlor, or individuals holding equivalent positions, as well as the beneficiaries or classes of beneficiaries, and any other natural person who exercises ultimate effective control over the arrangement. Sufficient information must be obtained to identify the beneficial owner when they intend to exercise their legally acquired rights.

Verification of Client Representatives or Agents

Lawyers must verify the identity of any person authorized to act or transact on behalf of a client, whether the client is a natural person or legal person. When confirming that the individual claiming to act on behalf of the client is duly authorized, the following types of documentation are generally acceptable:

1. A valid legal power of attorney.
2. A document from an official registry or other reliable source confirming ownership or legal representative status.
3. A court order or other official decision.

Due diligence procedures must be followed to identify and verify the identity of such individuals.

Enhanced Due Diligence

Lawyers and legal consultants shall apply enhanced customer due diligence measures to manage and mitigate risks associated with high-risk clients and transactions.

High-risk client

A high-risk client is one who poses elevated risk due to their personal profile, business activity, nature of the business relationship, or geographic location such as: clients from high-risk countries, non-residents who do not hold a valid identity card issued by the UAE, clients with complex ownership structures, clients conducting complex transactions with unclear economic or legal purpose, clients engaging in large cash transactions, clients transacting with unknown third parties, clients conducting transactions without face-to-face interaction, or any other client whom the lawyer reasonably determines to present high risk

Examples of Enhanced Due Diligence Measures are as follows:

1. Obtaining additional information and conducting inquiries into such information, including details about the client, the beneficial owner, and the purpose of the business relationship or transaction.
2. Updating client and beneficial owner due diligence information in a more systematic manner.
3. Taking reasonable measures to identify the source of funds of the client and the beneficial owner.
4. Increasing the level and frequency of ongoing monitoring of the business relationship and reviewing transactions to determine whether they appear unusual or suspicious.
5. Obtaining senior management approval prior to establishing a business relationship with the client.
6. When implementing these measures, lawyers shall pay particular attention to the reasonableness of the information obtained, and shall examine, assess, and identify any inconsistencies, contradictions, or circumstances that may be unusual or raise suspicion.

Politically Exposed Persons (PEPs)

Due to their potential influence over government policy, public funding decisions, procurement outcomes, or access to public funds, politically exposed persons are classified as high-risk individuals under the anti-money laundering and countering the financing of terrorism framework.

Federal Decree-Law No. (10) of 2025 defines politically exposed persons (PEPs) as:
A natural person who is or has been entrusted with prominent public functions in the UAE or in any other country, including heads of state or government, senior politicians, senior government officials, judicial or military officials, senior executives of state-owned enterprises, senior officials of political parties, and individuals entrusted with the management of international organizations or prominent positions therein. This definition also includes:

1. Immediate family members of the politically exposed person, including spouses, children and their spouses, and parents.
2. Known close associates of the politically exposed person, such as individuals who hold joint or sole beneficial ownership of a legal person or legal arrangement established for the benefit of the politically exposed person, or who maintain a close business relationship with them.

Lawyers shall establish appropriate risk management policies and procedures to determine whether a client or beneficial owner is a politically exposed person. In addition to standard due diligence procedures, lawyers are required to:

1. Take reasonable measures to identify the source of funds and source of wealth of the client or beneficial owner identified as a politically exposed person.
2. Assess the legitimacy of the source of funds and wealth, including conducting reasonable inquiries into the professional and financial background of the politically exposed person.
3. Obtain senior management approval prior to establishing a business relationship with the politically exposed person or continuing an existing relationship, and apply enhanced ongoing monitoring to such relationship.

In the case of domestic politically exposed persons and individuals who previously held prominent positions in international organizations, lawyers shall apply the above measures when the business relationship is classified as high-risk.

It is worth noting that potential risk factors include the level of (informal) influence the person may continue to exert, the seniority of the position previously held by the individual as a politically exposed person, and whether their former or current role remains connected in any way - for example, through the appointment of a successor to the politically exposed person, or through informal indications that the politically exposed person is still involved in the same substantive matters

High-risk countries:

Lawyers shall apply enhanced customer due diligence measures proportionate to the level of risk that may arise from business relationships or transactions involving a natural person or legal person from a high-risk country.

Law firms are required to implement the measures prescribed by the National Committee for Combating Money Laundering and the Financing of Terrorism in relation to high-risk countries.

High-risk countries are those classified as having significant strategic deficiencies in their national frameworks for combating money laundering, terrorism financing, and the financing of the proliferation of weapons. These countries are listed either on the internationally recognized list of high-risk jurisdictions issued by the Financial Action Task Force (FATF), or as designated by the National Committee for Combating Money Laundering and the Financing of Terrorism.

The list of high-risk countries may be accessed through the official website of the National Committee for Combating Money Laundering and the Financing of Terrorism.
https://namlcftc.gov.ae/en/
https://namlcftc.gov.ae/en/more/jurisdictions/high-risk-countries/

For further information, those seeking deeper insight into internationally recognized guidelines and standards in the field of anti-money laundering and countering the financing of terrorism may refer to the official website of the Financial Action Task Force (FATF):
https://www.fatf-gafi.org/

Simplified due diligence

Under certain conditions, and in the absence of any suspicion of money laundering or terrorism financing, law firms and legal consultancy offices may apply simplified customer due diligence measures with respect to clients identified as low-risk, based on a sufficient risk assessment. Simplified due diligence generally involves a more lenient application of certain aspects of the due diligence framework, proportionate to the identified low level of risk; examples include:

1. Verifying the identity of the client and the beneficial owner after the commencement of the business relationship.
2. Updating client information at less frequent intervals.
3. Reducing the frequency of ongoing monitoring and transaction reviews.
4. Inferring the purpose and nature of the business relationship from the type of transactions or the nature of the established relationship, without the need to collect specific information or perform defined procedures.

Ongoing Monitoring During the Business Relationship

Lawyers and legal consultants shall conduct ongoing monitoring of client activity, including reviewing and supervising executed transactions throughout the duration of the business relationship, to ensure consistency with the information available, the nature of the client's activities, and their risk profile. Where necessary, an investigation into the source of funds must be conducted.

A risk-based approach shall be used to determine the policies, procedures, and controls applied to monitoring client transactions and activities, including the extent of monitoring for specific clients or categories of clients.

Timely review and updating of simplified due diligence information is a key component of an effective framework for mitigating money laundering and terrorism financing risks.

Client records, including documents, data, and information relating to clients and their beneficial owners, must be maintained in an up-to-date and appropriate manner. This includes regular review of records, particularly for high-risk client categories, where information must be updated continuously and more frequently. In the case of low-risk clients, and where there is no suspicion of money laundering or terrorism financing, simplified due diligence information may be updated less frequently.

It is worth noting that, lawyers may, upon suspicion of criminal activity, refrain from applying customer due diligence measures if they have reasonable grounds to believe that such measures may alert the client. In such cases, the lawyer must submit a Suspicious Transaction Report (STR) to the Financial Intelligence Unit (FIU), clearly stating the reasons for not applying the due diligence procedures.

Exemption from Identifying Shareholders, Partners, or Beneficial Owners

Lawyers are exempt from identifying and verifying the identity of shareholders, partners, or beneficial owners when such information is obtained from reliable sources, in cases where the client or the controlling shareholder is a company listed on a regulated securities exchange subject to financial supervision and disclosure requirements; or a subsidiary whose majority shares or ownership interests are held by a parent company.

What should be done if Customer Due Diligence Measures cannot be applied?

Law firms and legal consultancy offices are prohibited from establishing or continuing a business relationship, or executing any transaction, if they are unable to apply customer due diligence measures. In such cases, they must submit a Suspicious Transaction Report (STR) to the Financial Intelligence Unit (FIU).

Third-party reliance

law firms and legal consultancy offices may, under certain conditions and in accordance with the controls set out in Article (20) of the Executive Regulations of Federal Decree-Law No. (10) of 2025, rely on a third party to carry out customer due diligence measures.

When relying on a third party, lawyers must promptly obtain from the third party the necessary identification data and other relevant information collected through due diligence procedures, and ensure that copies of the required documents can be obtained without delay upon request. Lawyers must also verify that the third party is subject to regulatory oversight and is committed to applying customer due diligence measures and maintaining records in accordance with the requirements of Federal Decree-Law No. (10) of 201825 and its Executive Regulations.

Ultimately, lawyers remain responsible for the accuracy and outcome of the due diligence process conducted on the client.

Appointment of a Compliance Officer

Law firms and legal consultancy offices are required to appoint a Compliance Officer under their responsibility, who possesses the appropriate competence and experience to carry out the following duties and functions:

1. Monitoring transactions related to criminal activity.
2. Reviewing records, receiving data on suspicious transactions, examining and assessing them, and deciding whether to report them to the Financial Intelligence Unit (FIU) or retain them with documented reasons, in strict confidentiality.
3. Reviewing internal systems and procedures for Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF), and assessing their consistency and compliance with the provisions of the Decree-Law and its Executive Regulations.
4. Evaluating the firm's adherence to systems and procedures for Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF), and recommending necessary updates and improvements.
5. Preparing semi-annual reports on these matters and submitting them to senior management, with a copy sent to the Anti-Money Laundering Department at the Ministry of Justice, including observations and decisions of senior management.
6. Establishing, implementing, and documenting ongoing training and qualification programs for the firm's staff on money laundering, terrorism financing, and Financing of the Proliferation of Weapons, and methods of prevention.
7. Cooperating with the Ministry of Justice, the Financial Intelligence Unit at the Central Bank, and other competent authorities in the UAE, by providing information and data and enabling their staff to access the necessary records and documents to perform their duties.
8. Verifying suspicious transactions, reporting them to the Financial Intelligence Unit, providing the required information, and cooperating as necessary with the Ministry of Justice and other competent authorities in the UAE.

The appointed Compliance Officer must meet the following conditions:

1. Must be at least twenty-one (21) years of age.
2. Must hold a qualification from a university or higher institute recognized in the UAE or its equivalent.
3. Must possess the appropriate competence and experience.
4. Must be fully legally competent, of good conduct and reputation, and must not have been convicted of a felony or a misdemeanor involving dishonesty or breach of trust, nor subjected to disciplinary action for any such offense.

In all cases, prior approval must be obtained from the Anti-Money Laundering and Counter-Terrorism Financing Department at the Ministry of Justice before appointing the Compliance Officer.

Reports of Suspicious Transactions or Activities

If a lawyer identifies grounds for suspicion or possesses reasonable cause to suspect a money laundering operation, they must report the matter directly to the Financial Intelligence Unit (FIU) without delay, via the electronic goAML system administered by the FIU.

A suspicious transaction refers to dealings involving funds that are suspected, or for which there are reasonable grounds to suspect, to be proceeds of any felony or misdemeanour, or linked to the financing of terrorism or financing of the proliferation of weapons -whether the transaction has been executed or merely attempted - regardless of its value or timing. Such transactions may include:

1. Proceeds of a crime (whether a felony or misdemeanor, committed within the State or in another jurisdiction that considers it a crime).
2. Transactions linked to money laundering, terrorist financing, or financing of the proliferation of weapons.
3. Transactions intended for use in activities associated with such crimes.

Lawyers and their staff must not, directly or indirectly, disclose to the client or any other person that the client has been reported to Financial Intelligence Unit (FIU), or that a report is about to be made, regarding the following matters:

1. A report has been prepared or is intended to be prepared.
2. Information or data contained in the report.
3. An investigation is underway regarding the transaction.

An attempt by the lawyer to dissuade the client from engaging in unlawful conduct shall not be considered a breach of confidentiality.

Reporting a suspicious transaction does not require proof that a predicate offense has occurred or that the proceeds originate from an unlawful source. It is sufficient to have reasonable grounds for suspicion, which may be inferred from:

1. Suspicious transactions or indicators thereof.
2. Transaction patterns or behavioral anomalies.
3. Customer due diligence information.

Confidentiality of Information

Lawyers must maintain the confidentiality of reported information and take reasonable measures to protect such data from unauthorized access. Law firms are required to establish adequate policies, procedures, and controls to ensure the confidentiality and protection of information related to suspicious transaction reports, including a documented procedure for reporting such transactions.

Law firms must define indicators that enable the identification of suspected criminal activity for the purpose of reporting suspicious transactions. These indicators must be regularly updated in line with evolving and diverse methods of criminal conduct, and in accordance with directives issued by regulatory authorities or the Financial Intelligence Unit (FIU) in this regard.

In cases of suspicion or when reasonable grounds exist to suspect that a transaction, attempted transaction, or funds - whether in whole or in part - constitute criminal proceeds, or are linked to or intended for use in criminal activity, the law firm must comply with the following obligations, without invoking banking secrecy, professional confidentiality, or contractual confidentiality:

1. Report the suspicious transaction directly to the Financial Intelligence Unit (FIU) without delay via the goAML electronic system.
2. Respond to any additional information requests made by the FIU.

Lawyers are exempt from reporting if the information concerning such transactions was obtained in the course of assessing the legal position of a client, defending or representing the client in judicial proceedings, arbitration, or mediation, or providing legal advice on matters related to such proceedings. This exemption applies regardless of whether the information was obtained before, during, or after the proceedings, or in other circumstances subject to professional confidentiality.

Neither the lawyer nor their staff shall bear any administrative, civil, or criminal liability towards the reported person when reporting to the Financial Intelligence Unit or providing information to the Unit in good faith.

Reporting Obligation

Each law firm and legal consultancy must designate a Compliance Officer who shall be responsible for reporting suspicious transactions to the Financial Intelligence Unit (FIU) via its electronic platform, goAML.

In addition, every lawyer or employee working within the law firm bears the responsibility of reporting any suspicious transactions to the designated Compliance Officer.

Accordingly, law firms are required to establish appropriate policies, procedures, controls, and training programs concerning internal reporting mechanisms. These mechanisms must enable managers and employees to report suspicious transactions (including the provision of necessary records and data) to the Compliance Officer for further analysis and decision-making in the context of Anti-Money Laundering, Countering the Financing of Terrorism (AML/CFT).

Reporting Timeline

The Executive Regulation stipulates that suspicious transaction reports must be submitted "without delay."
This means:

- All employees of the law firm must promptly report internally to the Compliance Officer whenever there is suspicion or reasonable grounds to suspect a transaction.
- The Compliance Officer must submit an external Suspicious Transaction Report (STR) to the Financial Intelligence unit (FIU) via the goAML system at the moment they determine that the transaction raises genuine suspicion and reporting thereof shall be mandatory.

Financial Intelligence Unit (FIU)

The Financial Intelligence Unit (FIU), operating under the Central Bank of the United Arab Emirates, is the official authority for financial intelligence.

The FIU functions independently under a legal and regulatory mandate as the national central authority and is solely responsible for, among other tasks:

1. Establishing and securing a database or registry of the information it receives, governed by rules ensuring information security and confidentiality.
2. Providing training courses and programs for qualifying its staff and other entities, both domestically and internationally.
3. Preparing studies, research, and statistics related to financial crimes, and monitoring relevant studies, researches, and statistics at the national and international levels.
4. Receiving reports from financial institutions and designated non-financial businesses and professions (DNFBPs), analyzing and storing them in its database using approved reporting formats.
5. Requesting additional information or documentation related to STRs and any other data it deems necessary from regulated entities and competent authorities, including customs disclosure information.
6. Forwarding STR-related data to national law enforcement agencies, judicial authorities, and public prosecution offices.
7. Exchanging information with counterpart FIUs in other countries pursuant to international agreements to which the UAE is a party, or through memoranda of understanding for the purpose of regulating mutual collaboration, subject to the principle of reciprocity where applicable.

Handling Transactions After STR Submission

Once the Compliance Officer submits a suspicious transaction report to the FIU, the law firm must comply with any instructions issued by the FIU. Additionally, the client must be immediately classified as high-risk, and appropriate enhanced due diligence and ongoing monitoring measures must be implemented until further guidance is received from the FIU.

Instructions issued by the FIU to the reporting law firm may include, but are not limited to:

1. Instructions to reject the transaction.
2. Instructions to proceed with the transaction (e.g., in cases of controlled delivery of funds to enable tracking by competent authorities).
3. Instructions to freeze or seize the client's funds or other assets.
4. Instructions to terminate the business relationship.
5. Instructions to maintain and monitor the business relationship, with periodic reporting of activities to the FIU and/or other competent authorities.
6. Requests for additional information regarding the reported transaction and other transactions linked to the client or the broader business relationship.

Law firms and legal consultancies must ensure confidentiality and full compliance with all instructions and requests issued by the FIU

Requirements Related to Emerging Technologies:

Lawyers and legal consultants shall remain abreast of modern technologies in the field of anti-money laundering, and in particular shall:

1. Identify and assess risks that may arise from the development of new products and professional practices, including new service delivery methods and the use of emerging or developing technologies for both new and existing products.
2. Evaluate such risks prior to launching or using any products, practices, or technologies, and implement appropriate measures to manage and mitigate those risks.

Recordkeeping Obligations

The law firm and legal consultancies shall establish transaction records that include the following:

1. All documents, records, and data pertaining to financial operations and commercial or cash transactions, whether domestic or international.
2. All documents obtained through customer due diligence measures, ongoing monitoring, account files, business correspondence, copies of personal identification documents, including suspicious transaction reports and the results of any analysis conducted.
3. Records, documents, and files shall be maintained in an organized manner that enables data analysis and the tracking of financial transactions.

Records Retention Period

Law firms and legal consultancy offices shall retain such records for a minimum period of five (5) years in the following cases:

1. From the date of completion of the transaction.
2. Upon termination of the business relationship with the client.
3. Upon termination of the business relationship.
4. From the date of account closure for clients.
5. Upon completion of a one-off transaction.
6. From the date of completion of inspection by the relevant department.
7. From the date of conclusion of an investigation.
8. From the date of issuance of a final judgment by the competent judicial authorities.

All of the above shall apply as appropriate.

Availability of Information and Records

The law firm and legal consultancies shall make all client-related information pertaining to customer due diligence, ongoing monitoring, and the results thereof - along with all relevant records, files, documents, correspondence, and associated forms - immediately available to the competent authorities upon request.

Training and Awareness Raising

To ensure the effectiveness of risk assessment and mitigation measures related to money laundering and terrorism financing, the law firm and legal consultancies shall ensure that all its employees have a clear understanding of the risks associated with money laundering and terrorism financing, and are aware of the appropriate procedures and decisions to be taken in the event of attempted exploitation or suspicion regarding a client, transaction, or activity.

Furthermore, given the evolving nature of money laundering and terrorism financing crimes, law firms and legal consultancy offices must ensure that their staff remain continuously informed of the latest developments, including new risks and both internal and external threats. In addition, training records shall be maintained and made available to Ministry of Justice inspectors upon request.

To be effective, the training program shall not be limited to explaining laws and regulations related to combating money laundering and terrorism financing, but shall also include internal policies and procedures used to mitigate and assess risks, as well as understanding the responsibilities and duties of lawyers under the applicable legislation.

It is worth noting that the Anti-Money Laundering Department at the Ministry of Justice develops an annual training plan and organizes a variety of specialized workshops and training courses in cooperation with relevant entities. All lawyers, legal consultants, and staff of law firms and legal consultancy offices are invited to participate in these sessions to ensure general awareness is raised. Most of these workshops and courses are offered free of charge.

Targeted Financial Sanctions

The term *targeted sanctions* refers to sanctions that are strategically focused on specific individuals, entities, groups, or institutions.

The term *targeted financial sanctions* refers to asset freezing measures and prohibitions on making funds or other assets available - whether directly or indirectly - for the benefit of individuals, entities, groups, or institutions subject to sanctions.

What is the Purpose of Targeted Financial Sanctions?

The purpose of targeted financial sanctions is to deprive certain individuals, groups, institutions, and entities of the means of supporting terrorism or financing the proliferation of weapons of mass destruction. To achieve this, targeted financial sanctions aim to ensure that no funds, financial assets, or economic resources of any kind are made available to such persons or entities while they remain subject to these measures.

Law firms and legal consultancy offices shall undertake the following:

1. **Registration** with the Executive Office for Control and Non-Proliferation to receive automatic notifications via email.
   This registration is intended to assist law firms and legal consultancy offices in receiving timely and updated information regarding the inclusion or removal of individuals from the local and UN sanctions lists.
2. **Screening:** Conduct regular and periodic checks of the following databases to identify potential matches with names listed on UN or local sanctions lists, including:
   A. Client databases
   B. Names of parties to any transactions
   C. Prospective clients
   D. Beneficial owners
   E. Names of individuals or entities with direct or indirect relationships
   F. Clients prior to executing any transaction or entering into any serious business relationship
3. **Implementation of freezing measures** without delay (within 24 hours) and without prior notice to the listed individual or entity, immediately upon identifying a match during the screening process.
4. **Notification to the Executive Office for Control and Non-Proliferation** within one (1) business day of implementing the freezing measures, along with all relevant supplementary information.

5. **Establishment and enforcement of:**
    A. Internal controls and procedures to ensure compliance with the obligations arising from this resolution.
    B. Policies and procedures prohibiting employees, directly or indirectly, from informing the client or any third party that a freezing measure or other sanction-related action will be implemented pursuant to this resolution.
    C. Through these internal controls, policies, and procedures, each law firm may define its own operational practices for implementing these measures, taking into account the nature of its business and clientele.
6. **Cooperation with the Executive Office for Control and Non-Proliferation** in verifying the accuracy of the information provided.

Types of Targeted Financial Sanctions

There are two main types of targeted financial sanctions:

1. Asset Freezing: Asset freezing refers to the prohibition of transferring, converting, disposing of, or moving any funds or other assets owned or controlled by individuals, groups, or entities listed on the sanctions list. This includes:
    A. Freezing of funds and other financial assets and economic resources, including prohibiting their use, alteration, movement, transfer, or access.
    B. Freezing of economic resources, which also includes prohibiting the acquisition of funds, goods, or services in any form, including but not limited to selling, leasing, or pledging them.
2. Prohibition on Making Funds Available: This refers to the prohibition on making funds available or providing financial or other services to individuals, groups, or entities listed on the sanctions list. This includes, for example, opening bank branches in jurisdictions subject to sanctions or providing financial services.

International and domestic sanctions Lists

Cabinet Resolution No. (74) of 2020 concerning the Terrorism Lists System and the implementation of United Nations Security Council resolutions related to the prevention and suppression of terrorism and its financing, as well as the prevention of the proliferation of weapons and its financing, and related resolutions, includes two types of sanctions lists applicable to individuals and entities:

1. The UAE Domestic Terrorism List issued by the Cabinet

   This list includes the names of individuals, entities, and organizations that have committed, planned, promoted, or financed terrorist activities.

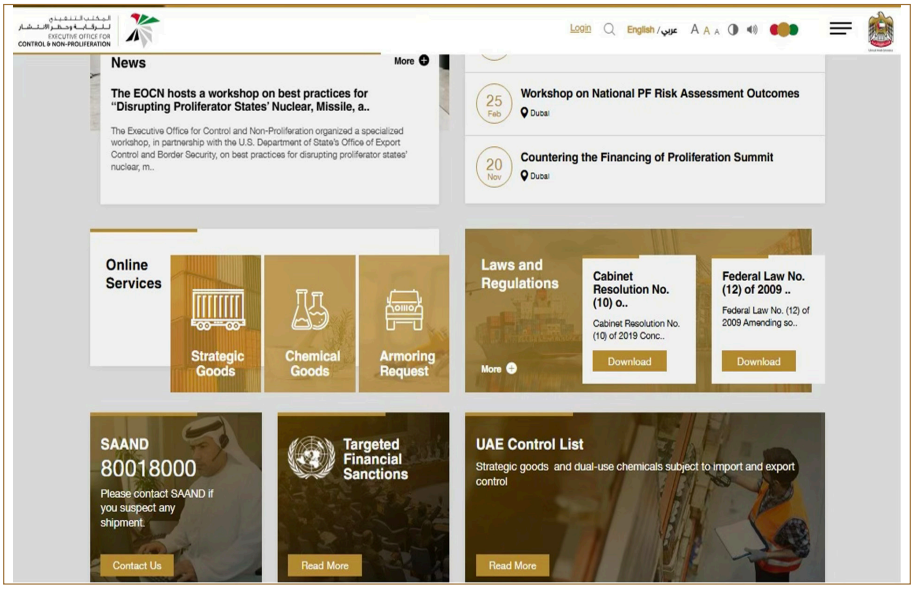
2. The United Nations Security Council Sanctions List

   - This list contains the names of individuals, entities, and organizations designated by the United Nations as engaging in activities that threaten development and peace.
   - These names are often implicated in acts of terrorism, genocide, and violations of international law. The list can be accessed via the following link https://www.un.org/securitycouncil/content/un-sc-consolidated-list
   - It is also worth noting that the United Nations Security Council Sanctions Lists and the UAE Domestic Terrorism List can be accessed by browsing the official website of the Executive Office for Control and Non-Proliferation: https://www.uaeiec.gov.ae/en-us/

   - It should be noted that these lists are subject to continuous updates, including the addition, removal, or modification of names. Accordingly, lawyers are required to conduct regular screenings of both lists, as well as upon receiving any notifications of amendments or updates.
   - Subscription to email notifications via the website of the Executive Office for Control and Non-Proliferation is recommended to ensure timely receipt of the latest updates to the lists.

- Before law firms and legal consultancy offices engage with a new client or enter into any transactions, they must review the full requirements of the Targeted Financial Sanctions Program, as well as the published lists of known or suspected terrorists, drug traffickers, and other criminal actors, to identify any potential matches.
- Lawyers are obligated to conduct periodic screening and verification of the client database - covering current, new, and prospective clients - to detect any matches with listed individuals. The database must also be re-screened whenever new names are added to the lists, and such screening must be carried out without delay.
- The term "without delay" shall mean within hours of the designation (listing) by the United Nations Security Council or the Cabinet of the United Arab Emirates

The electronic platform of the Executive Office for Control and Non-Proliferation (EOCN).



The electronic platform maintained by the Executive Office for Control and Non-Proliferation (EOCN), dedicated to publishing sanctions lists issued by the United Nations Security Council and the UAE Cabinet, offers several advantages, including:

1. Registration of all supervisory authorities on the platform to receive immediate updates regarding the UN Security Council Sanctions List and the UAE Domestic Terrorism List, along with the ability to provide feedback if information is available about listed individuals or entities.
2. Real-time access for all entities to view the latest updates to the sanctions lists at any time.
3. Explanation of the grievance procedures available on the platform for listed individuals residing in the UAE.
4. Open subscription for any user to receive notifications regarding updates to the sanctions lists.

For inquiries, the Executive Office for Control and Non-Proliferation may be contacted via the following email. iec@uaeiec.gov.ae

Proliferation Financing

Federal Decree-Law No. (43) of 2021 concerning goods subject to non-proliferation controls aims to prevent the unauthorized and illicit trade in dual-use goods that contribute to the production or development of weapons of mass destruction (WMD), related technologies, and their means of delivery.

The above-mentioned Decree-Law defines non-proliferation as "the prevention of unauthorized and illicit trade in goods that contribute to the production or development of weapons of mass destruction, related technologies, and their means of delivery."

The term *proliferation of weapons of mass destruction* refers to the manufacture, acquisition, possession, development, export, cross-border shipment, brokering, transfer, movement, storage, and use of nuclear, chemical, or biological weapons, their delivery systems, and associated materials. It also includes dual-use technologies and goods exploited for unlawful purposes.

The term *proliferation financing* refers to the risk of raising, moving, or generating funds, other assets, or economic resources - or the full or partial financing of individuals or entities - for the purpose of proliferating weapons of mass destruction, including the dissemination of delivery methods or associated materials. This also encompasses dual-use technologies and goods exploited for unlawful ends.

The Executive Office for Control and Non-Proliferation (EOCN) serves as the central authority in the United Arab Emirates responsible for ensuring the implementation of targeted financial sanctions. It is also the designated licensing authority for reviewing applications related to the import, export, re-export, and transfer of controlled goods, information, and technologies to, from, and through the UAE.

The Executive Office for Control and Non-Proliferation (EOCN) works closely with supervisory authorities to ensure a proper understanding of proliferation and proliferation financing risks faced by the private sector, and to ensure the effective implementation of targeted financial sanctions and other obligations related to proliferation financing.

Law firms must review the guidance and directives issued by the Executive Office for Control and Non-Proliferation (EOCN)in its capacity as the competent authority for implementing the provisions of Federal Decree-Law No. (43) of 2021 concerning goods subject to non-proliferation controls, which aims to prevent unauthorized and illicit trade in goods that contribute to the production or development of weapons of mass destruction and related technologies and means of delivery.

Law firms are also required to update their internal policies, procedures, and controls to include operational components aims at assessing and mitigating proliferation and proliferation financing risks. This should be based on data analysis derived directly from the nature of their business, client profiles, and the scope of services provided. Most importantly, firms must fully comply with the guidelines of the Financial Action Task Force (FATF) on countering proliferation and proliferation financing, which can be accessed via https://www.fatf-gafi.org.

Stages of Proliferation Financing

Proliferation financing may occur through three main stages, as follows:

Stage One: Fundraising for Armament Programs

A country with an armament program raises financial resources to cover domestic costs. Funding sources may include the national budget allocated to armament programs, as well as profits generated from networks of commercial companies abroad and proceeds from criminal activities conducted internationally.

Stage Two: Obfuscation of Funds

In this stage, a country with armament programs transfers assets into the international financial system, often involving foreign currency exchange transactions for trade purposes. The country may employ a range of methods - from simple to complex - using conventional correspondent banking channels or a sophisticated network of supply agents and front companies. At this stage, countries subject to comprehensive sanctions seek to circumvent those sanctions by employing advanced techniques to conceal the origin and movement of funds.

Stage Three: Procurement of Materials and Technologies

In this stage, the country with armament programs - or its agents - uses obfuscated resources to procure materials and technologies through the international financial system. This includes making payments for the shipment and transfer of such materials and technologies.

We advise Designated Non-Financial Businesses and Professions (DNFBPs) - particularly law firms, legal consultancies, and legal researchers - to consult the guidance materials available on the official website of the Executive Office for Control and Non-Proliferation https://www.uaeiec.gov.ae/en-us/ for further information on proliferation financing and related topics, especially those concerning evasion of targeted financial sanctions. The website offers a distinguished collection of guidelines, advisories, and training materials across various relevant topics, available in both Arabic and English.

Administrative Sanctions

The Anti-Money Laundering Department shall, upon identifying violations during inspections of law firms, legal consultancies, or notary offices with respect to any provisions of the Federal Decree-Law, its Executive Regulations, or decisions issued pursuant thereto, undertake the following procedures:

1. Notifying the violator regarding the alleged violations. The violator must implement corrective measures and submit supporting documentation within the timeframe specified by the Department.
2. Upon expiry of the specified period, the Department shall review the violator's response and the submitted documents, and assess the appropriate action; either by accepting the response or referring a report to the Undersecretary.
3. If a report is submitted to the Undersecretary, it must include a statement and identification of the alleged violations, the violator's response (if any), and the Department's recommendation regarding the appropriate action.
4. The Department may submit a report directly to the Undersecretary without considering the corrective measures taken by the violator in any of the following cases:
    A. Repetition of a previously corrected violation identified during a prior inspection.
    B. Clear breach of governance systems within the law firm or legal consultancy.
    C. Serious breach of anti-money laundering and countering the financing of terrorism procedures.
5. Upon confirmation of a violation, a reasoned decision shall be issued by the Undersecretary imposing one or more of the following administrative sanctions:
    A. Warning.
    B. Administrative fine.
    C. Prohibition from working in the relevant sector for a period specified in the decision.
    D. Restriction of powers of managers found responsible for the violation; the decision may include appointment of a temporary monitor.
    E. Suspension of managers found responsible for the violation for a specified period, or request for their replacement if permissible.
    F. Suspension or restriction of professional practice for a specified period
    G. Revocation of license.
6. Except for license revocation (paragraph G), the Department may request the submission of regular reports on corrective measures taken to remedy the violations.
7. The Anti-Money Laundering and Counter-Terrorism Financing Department shall notify the violating law firm and legal consultancy office of the sanction decision within twenty (20) business days from the date of issuance.

    The Department may also publish the imposed administrative sanctions through various media outlets.

Appealing Administrative Sanctions

An appeal against a decision imposing an administrative sanction may be submitted within thirty (30) business days from the date of notification or awareness of the decision, as applicable. The appeal must be substantiated and accompanied by all supporting documentation, and shall be submitted to the Minister of Justice. Failure to receive a response to the appeal within forty (40) business days from the date of submission shall be deemed a rejection of the appeal.

No legal challenge against the decision to impose an administrative sanction shall be accepted unless an appeal has first been submitted and either rejected or the response period has lapsed. The decision issued in response to the appeal shall be final.

Criminal Penalties

Federal Decree-Law No. (20) of 2018 sets forth a range of criminal penalties related to money laundering and terrorism financing offenses. Accordingly, lawyers and legal consultants must be fully aware of and familiar with the penalties applicable in cases of non-compliance with the obligations imposed by law.

Sources of Assistance and Additional Information

Combating money laundering and terrorist financing is inherently complex, dynamic, and subject to constant change. Therefore, Designated Non-Financial Businesses and Professions (DNFBPs) must ensure that their compliance officers and staff remain informed of developments in this field. To support this objective, the following sources of additional information are provided:

- National competent authorities, including the Ministry of Justice, the National Committee for Anti-Money Laundering, Countering the Financing of Terrorism and Countering Proliferation Financing (AML/CFT/CPF), and the UAE Financial Intelligence Unit (FIU).
- Websites of international bodies, such as the Financial Action Task Force (FATF), the Middle East and North Africa Financial Action Task Force (MENAFATF), and other FATF-style regional bodies.
- The official website of the United Nations Office on Drugs and Crime (UNODC).
- For further assistance, the Anti-Money Laundering and Counter-Terrorism Financing Department at the Ministry of Justice may be contacted via email at amlctf@moj.gov.ae. In addition, a dedicated direct line is available at: 02 692 1660.
- Additionally, the Ministry of Justice website https://www.moj.gov.ae/en/home.aspx features a dedicated page for the Department, providing access to key legislation, relevant decisions, guidance materials, and important links to assist law firms and legal consultancy offices in accessing information efficiently.

Judge/ Dr. Abdullah Ahmad Al-Rashed

Director, Anti-Money Laundering and
Counter-Terrorism Financing Department
25/11/2025