The Guideline

For licensed practitioners of the law profession and notarization regarding the fight Against Money Laundering (AML), Terrorism Financing (TF), and the Proliferation Financing (PF)

2025

Contents

Introduction: Regulatory context, definitions, and general framework

Introduction and Objective

- Overview of the contents of the guideline and its objectives
- The role of the Ministry of Justice (MOJ) as the supervising authority

Penalties and Enforcement of the law

- Compliance and risk-based monitoring
- What is meant by Terrorism Financing (TF)?
- What is meant by the Proliferation Financing (PF)?
- What is meant by Money Laundering (ML)?
- The risks faced by lawyers and notary officers

First: Responsibility and governance

Second: Risk-Based Approach (RBA)

- Integration and comparison of risks
- Risks of service delivery channels
- Country risk

Third: Due Diligence towards Clients (CDD) and monitoring

- Due diligence for individuals
- Risk-based due diligence towards clients
- Verification
- Beneficial ownership
- Client risk assessment
- Identity verification

Suspending operations and reporting suspicious transactions

Fourth: Reporting suspicious transactions (and internal reporting)

Third: Due Diligence towards Clients (CDD) and monitoring

- Due diligence for individuals
- Risk-based due diligence towards clients
- ✓ Transactions
- ✓ Monitoring based on the existence of requirements
- ✓ Periodic monitoring
- Client risk assessment
- Identity verification
- Verification
- Beneficial ownership

Fifth: Record keeping

- When should training be completed?
- What should training include?
- . Training and awareness

Introduction: Regulatory context, definitions, and general framework

Introduction and Objective

- Lawyers and notary officers are key gatekeepers for the financial system and trade, facilitating vital transactions and information that underpin the Kingdom of Saudi Arabia's economy. As such, they have a significant role to play in ensuring their services are not used to further a criminal purpose. The fight against crime demands that criminals be prevented from legitimizing the proceeds of their crime by the process of "Money Laundering" which often involve entities considered outside traditional targets, such as banks, credit institutions, and money exchangers. Licensed professionals such as lawyers and notary officers are exposed to the risk of their work being exploited to facilitate those prohibited transactions by ML perpetrators , TF or PF of mass destruction, who often seek to involve other parties without their knowledge.
- This guidelines is based on the relevant Law and Implementing Regulations. This Guidance aims to cover activities that fall within the scope of the law, including the practice of law and notarization, concerning the client's purchase, sale, or leasing of real estate, and managing the client's funds, including their bank or investment accounts or other assets, establishing, operating or managing legal entities, arrangements, or organizing related subscriptions, and the client's purchase or sale of commercial companies. This is in accordance with the powers stipulated by law, and in accordance with the provisions of the AML law , the Combating Terrorism Crimes and its Financing Law, and their Implementing Regulations.

The Role of the Ministry of Justice (MOJ) as the Supervising Authority

MOJ is the supervisory body responsible for overseeing the offices of licensed professionals practitioners of law and notarization, according to the provisions of (Chapter Nine) of the CTF Law, and (Chapter Six) of the AML Law, and is responsible for the following tasks:

- Registering licensed professionals according to the legal conditions and requirements.
- Monitoring and acting to ensure compliance of licensed professionals with the activities within the scope of the AML Law and the CTF Law and their IMs.
- Issuing relevant guidelines, instructions, and procedures.

Overview of the Guideline's Contents and its Objectives

- MOJ issues this guidelines to promote compliance with the AML Law and its Implementing Regulations, the CTF Law and its Implementing Regulations, and compliance with the requirements to CTF
- Where this guidance identifies high risk of ML or TF, licensed professionals are required to apply EDD in those cases.
- MOJ may consider whether licensed professionals have complied with this Guidelines in the following cases:

1. To determine whether to take enforcement action or impose a penalty under the AML Law or the CTF Law or their Implementing Regulations.
2. 9. As a relevant factor in the level of fines to be imposed in the event of breach of the AML Law or the CTF Law or their Implementing regulations.
3. A court determining an allegation of a breach of the law or Regulations may take account of whether the the licensed professional complied with this Guidance.
4. If a professional body is called upon to judge whether a member has complied with its general professional conduct, it may be influenced by whether the member has applied the provisions of this guidance.

- Note that the Saudi Arabia Financial Intelligence Unit (SAFIU) under the Presidency of State Security is an important institution as it is a specialized entity, receive reports and notifications regarding suspicious operations, issues guidelines in this regard that must be referred to and verified for application, but it is not considered a supervisory authority within the meaning in (Chapter Nine) of the CTF Law, and (Chapter Six) of the AML Law.
- Wherever this guide refers to entities, it applies to individual licensed professionals, and vice versa, unless the context requires otherwise.

Penalties and Enforcement of the Law

The AML Law and the CTF Law stipulate granting supervisory authorities the power to impose a number of administrative financial penalties on licensed professionals who violate the provisions of those Laws and their Implementing Regulations in accordance with what is stipulated in Article 25of the AML Law and Article 83 of the CTF Law.

What is meant by Money Laundering (ML)?

- Money laundering includes all forms of using or possessing funds obtained from illegal sources to facilitate their use or possession regardless of how it were obtained through concealing the illegal source of those funds. Article 2 of the AML Law stipulates a number of acts that constitute money laundering as follows:

1. Transferring,moving money or conducting any operation with it, knowing that it is the proceeds of a crime; to conceal the illegal source of that money, to disguise it, or to assist any person involved in committing the original crime from which that money was obtained to escape the consequences of committing it.
2. Acquiring, possessing, or using money, knowing that it is the proceeds of a crime or an illegal source.
3. Concealing the nature of money, thier source, movement, ownership, location, or methods of disposal, or rights associated with them, knowing that they are proceeds of a crime.
4. Attempting to commit any of the acts specified in paragraphs (1), (2), and (3) - mentioned above - or participating in committing them through agreement, securing assistance, incitement, providing advice, guidance, counsel, facilitation, collusion, concealment, or conspiracy.

- Despite the variety of methods employed, the laundering process is typically accomplished in three stages which may comprise numerous transactions by the launderers that could raise suspicions of underlying criminal activity:

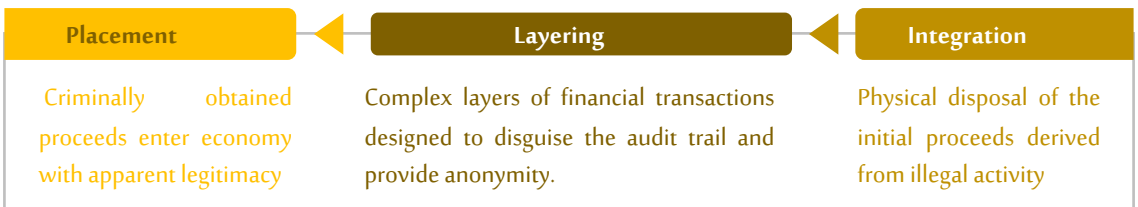


Figure 1: Stages of Money Laundering | The three basic steps may occur separately and distinctly, or they may occur simultaneously or overlap.

The Risks faced by Lawyers and Notary Officers

- It is difficult to distinguish between the activities of those engaged in commercial money laundering and the activities carried out by clients. Like the legitimate client, the launderer may need legal services and a whole range of financial, tax and business advice and support. Some areas of a lawyer's work and notary officers may be more vulnerable than others to the involvement of money launderers, but no area is immune.
- Criminal proceeds can take many forms. Cost savings (as a result of tax evasion or ignoring legal requirements) and other less obvious benefits can be proceeds of crime. Where criminal property is used to acquire more assets, these too become criminal property.
- If someone knowingly engages in criminal activity, but fails in benefitting from it, then he may have committed some offence other than money laundering (it will often be SAFIU) and firms and individuals should nonetheless consider whether they are under some other professional reporting obligations. Lawyers and notary officers can benefit from the following illustration.

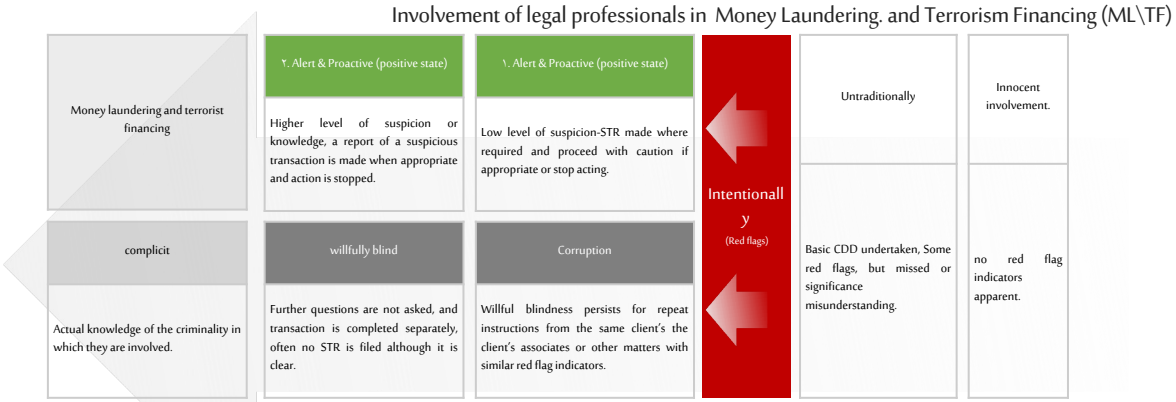


Figure (2): Financial Action Task Force FATF report titled "Vulnerabilities of Legal Professions to Money Laundering and Terrorist Financing" – June 2013

- Criminal property can take any form, including:
  - A. Cash or equivalents.
  - B. Securities.
  - C. Reducing financial liabilities.
  - D. Tangible or intangible assets.
- For the purposes of this guidance money laundering also includes terrorist and proliferation financing.

What is meant by Terrorism Financing (TF)?

Before stating the meaning of the financing of terrorism,It is important to clarify what is meant by the terrorist crime first; paragraph (3) of Article 1 of the CTF Law defines the crime of terrorism as Any act committed, individually or collectively, directly or indirectly, by a perpetrator to disturb public order, destabilize national security or State stability, threaten national unity, suspend the Basic Law of Governance or some of its provisions, cause damage to State facilities or natural or economic resources, attempt to coerce any of its authorities into a particular action or inaction, cause harm or death to any person, when the intention of such act, by its nature or context, is to terrorize people, force a government or an international organization to commit or refrain from committing a certain act, or threaten to carry out acts that would lead to or instigate any of the aforementioned intentions. It shall also refer to any act that constitutes a crime under international conventions or protocols on terrorism or terrorism financing, to which the Kingdom is party, or any of the acts listed in the Annex to the International Convention for the Suppression of the Financing of Terrorism. Accordingly, the crime of financing terrorism, according to what is included in paragraph (4) of Article 1 of the Combating Terrorism Crimes and its Financing Law, is Providing funds for committing a terrorist crime or for supporting a terrorist entity or a terrorist individual in any form stipulated in this Law, including financing the travel and training of a terrorist

individual.

- It is worth noting that financial gain is the primary objective in all types of financial crimes. Nonetheless, terrorist groups, such as: Criminal organizations need to develop sources of funding and means to launder that money and use it to obtain the materials and logistical means necessary to carry out terrorist acts.
- Sources of funding terrorist can be illicit sources, such as: Kidnapping, extortion, smuggling, various types of fraud, theft, robbery, drug trafficking, CD piracy, forgery, cigarette smuggling, credit card fraud, small-scale drug trade. Lawyers and notary officers must be aware however, that funding for terrorist groups, unlike for criminal organizations, may also include funds derived from legitimate sources or from a combination of lawful and unlawful sources. This funding from legal and legitimate sources is a key difference between terrorist groups and traditional criminal organizations.

- Terrorist groups find ways of laundering the funds to disguise links between them and their funding sources, and to be able to use the funds without attracting the attention of authorities.
- Charities or other non-profit organizations (NPOs) are also vulnerable to exploitation and can be misused for TF; terrorist groups use NPOs to raise and launder funds to finance terrorist activities.
- Any person who believes or suspects that another person has committed an offence under the CTF law must disclose the information to the SAFIU or to the police as soon as is reasonably practical. Failure to do so is a crime by law and is punishable.

What are Targeted Financial Sanctions?

Lawyers and notary officers have obligations under various international targeted financial sanctions or orders, as well as classifications and guidelines issued regarding TF and PF, when applicable. United Nations and national sanctions are implemented in the Kingdom of Saudi Arabia, and establishments must take the necessary measures accordingly.

What is meant by the Proliferation Financing (PF)?

PF refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, storage or use of nuclear, chemical, radiological or biological weapons and their means of delivery and related materials (including both technologies and dual use of goods used for illicit purposes). CTF Law criminalizes all operations that involve support or funding contributing to the unlawful proliferation of weapons; Article 36 of the law stipulates that anyone who commits any of the crimes specified in the law shall be punished by imprisonment for a period not exceeding (twenty) years and not less than (ten) years, if they commit any of the following acts: (train or trained by or funded training on any of the following:

A- The use of any weapons, explosives, nuclear, chemical, biological, or radiological materials, poisons, incendiary devices, or any means of wired or wireless or electronic communication, or their manufacture, preparation, assembly, development, provision, possession, storage, or bringing, as stated in Article 37 of the same Law, any person who provides a terrorist entity, a member thereof, or any terrorist

individual with weapons; explosives; ammunition; nuclear, chemical, biological, radioactive materials; poisons; or incendiary devices, shall be subject to imprisonment for a term not exceeding 30 years and not less than 10 years. Similarly, Article 39 of the same system stipulates that any person who smuggles weapons; ammunition; explosives; nuclear, chemical, biological, radioactive materials; poisons; incendiary devices; any means of wired, wireless, or electronic communication; or manufactures, develops, assembles, prepares, imports, acquires, or possesses the same; smuggles any parts, raw materials, or devices used in their manufacturing,preparation or equipment; or transports the same by mail, public or private transportation, or any other means with the intent to commit any of the crimes stipulated in this Law, shall be subject to imprisonment for a term not exceeding 25 years and not less than 15 years.

Compliance and risk-based monitoring

First: Responsibility and Governance

- Good governance in law and notary firms and is essential for effective internal controls.
- For Firms conducting activities in scope, the Implementing Regulations require laws and controls to mitigate and manage ML, TF, PF risk and ensure compliance with TFS. The Regulations impose a duty to ensure that relevant staff are kept aware of these controls and are trained to apply them properly.
- If a firm fails to meet its obligations under the AML Law or the CTF Law or their Implementing Regulations, penalties may be imposed on it and on any individuals deemed responsible. This could include anyone in a senior position who neglected their own responsibilities or agreed to something that resulted in the compliance failure.

Systems and Controls

The Implementing Regulations of the AML Law and the CTF Law impose obligations on law and notary firms to adopt measures and procedures for internal control. These provisions apply to individual practitioners, who must document this control to prove it to the MOJ within this guideline. The reference to control can be interpreted to include written policies and procedures or systems to mean various control means that work together.

Second: Risk-Based Approach (RBA)

Lawyers and notaries must focus resources and controls on areas of higher risk, RBA and adapt their response according to their perceptions of risk. Thus, risks are identified and then risk-based control provisions are applied for CDD and monitoring.

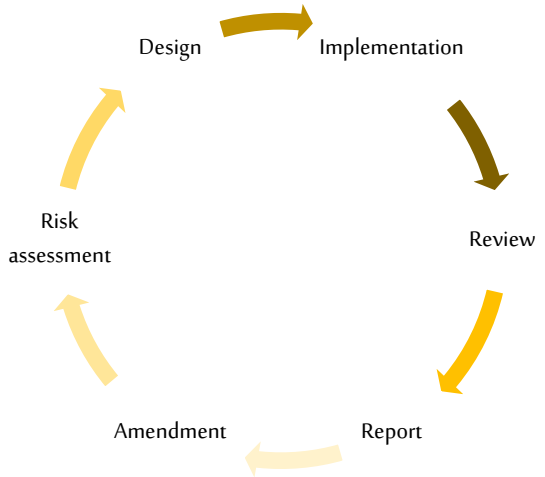
"Clients Risks"	(A) Client of the person
"Country Risks"	(B) The country or geographical area in which the client resides or operates
"Service Risks"	(C) The products, services, and transactions of the person.and
"Service Delivery Channel Risks"	(D) The delivery channels of the person
You must:	
(a) Document the person's risk assessments.	
(b) Consider all relevant risk factors before determining the overall risk level and the appropriate level and type of mitigation to be applied.	
(c) Keep the person's risk assessments up to date.	
(d) Maintain appropriate mechanisms to provide risk assessment information to competent authorities and self-regulatory bodies.	
(e) Implement policies, controls, and procedures approved by senior management to enable the person to manage and mitigate risks identified by the country or from covered activities.	
(f) Identify and assess money laundering or terrorist financing risks that may arise in connection with the development of new products and new business practices, including new delivery mechanisms and the use of new or advanced technologies for both new and existing products.	
(g) Monitor the implementation of the controls referred to in paragraph (e) and enhance controls as necessary.	
(h) Take enhanced CDD measures with customers to manage and mitigate risks when higher risk is identified.	

- RBA is fundamental and requires an analysis of the risks of ML, TF, and PF faced by law and notary firms to take appropriate responses.
- RBA is the foundation of AML and TF procedures for any entity.
- RBA supports evidence-based decision-making to better target risks.
- Controls will not be able to detect and prevent all ML activities, but a realistic analysis of actual risks enables the entity to focus greater resources on the largest threats.

Business Risk Assessment (BRA)

There is a requirement for lawyers and notaries to conduct BRA and Client risk assessments.The BRA linked to the firm's business plan and , leading to decisions on the entity's risk acceptance or tolerance to be included in other risk assessments related to the feasibility of the entity's business plans and potential liabilities.

- Deciding to offer activities within the scope of services increases the entity's exposure to ML/TF/PF risk , placing it under the scope of supervision according to the Implementing Regulations (referred to as regulatory risk). Therefore, the entity must identify and assess both the risks and how it will address them through its operations and the controls it applies.
- The vital component is the business data used to identify and assess risks, which typically change over time, and lawyers and notaries must periodically review and update the assessment (recommend annually and upon the occurrence of significant events).
- RBA does not exempt low-risk clients, services and situations from AML/CFTP/TFS procedures, rather procedures may be less burdensome than those believed to represent a lower level of risk.
- The Firm must ensure that that the analysis of ML TF PF risks is conducted by identifying their nature and severity identified and assessing them to produce an accurate risk profile and then taking action to mitigate those risks in proportion to the severity of the threats they pose.
- Where a ML TF PF risk is identified, the Firm must design and implement appropriate procedures to manage it. The reasons for believing that these measures are appropriate must be supported by documented evidence and systems established to monitor effectiveness.



- ML, TF, and TP risks include the possibility that the entity may:

a. be used for money laundering (e.g. by holding criminal proceeds in a client money account or or by engaging in arrangements that conceal the true beneficiaries of criminal proceeds);

b. used to facilitate money laundering by another person (e.g. by creating a a legal entity in money laundering or by introducing a money launderer to another organized entity);

C. suffering consequential legal, regulatory, or reputational damage as result of a client's involvement in money laundering.

- The risk profile of any Firm changes over time along with the business and its operating environment. The risk analysis should be refreshed regularly, the frequency of which should reflect the ML/TF/PF risks faced by the firm and the stability or otherwise of the business environment. A fresh analysis may then require AML/CTF/CPF procedures to be amended and fed into the review of the System. The Firm may already have general risk analysis processes, and these could form the basis of its ML/TF/PF risk analysis
- Risks are grouped into categories: 'client', 'service', 'geography' and 'delivery channels' but don't look at individual risks in isolation. When two threats are combined they can produce a total risk greater than the sum of the parts.
- The risk assessment of the Firm should show where risks are likely to arise, and so where certain controls will be needed to tackle them.

Client Risks

- Client risk is the MLTFPF risk posed by a client. The Firm should ask itself "Does our client have attributes known to be frequently used by money launderers or terrorist financiers?"
- Firms should have different client risk ratings such as low, normal/medium, and high.
- The following may suggest a high risk of money laundering or terrorist financing.

A- Undue client secrecy (e.g. reluctance to provide requested information)

b. Unnecessarily complex ownership structures (including nominee shareholders or bearer shares);

c. Underlying Business activities:

1. cash-based businesses;

2. money service bureaus;

3. arms dealers;

4. property transactions with unclear source of funds; .

d. Resident or national of high-risk country

e. politically exposed person;

f. new clients carrying out one-off transactions;

g. rapid rate of turnover (i.e., trades for a short period of time, close and then starts up as a new company)

h. client is taking on work which is outside its normal range of goods and services;

i. clients that are involved in transactions that don't make commercial sense or involved in transactions where the source of funds is unusual or unknown;

j. high net worth individuals;

k. uncooperative clients;

l. clients who have known criminal convictions relating to the proceeds of crime;

m. the client's lifestyle and/or transactions are inconsistent with known business and personal information;

n. the client has multiple bank accounts or foreign accounts with no good reason;

o. the client has changed professional advisors several times in a short space of time without legitimate reasons,

p. the service being requested was refused by another professional advisor without legitimate reasons, or

q. the client is prepared to pay substantially higher fees than usual without legitimate reasons.

r. The client is listed under Security Council sanctions..

Service Risks

- Service risk is the perceived risk that certain services present an increased level of vulnerability to being used for ML TF PF purposes. The Firm should ask itself "Do our services have attributes known to be used by money launderers or terrorist financiers?"
- Services in which there is a serious risk that the Firm itself could commit a ML crime should be treated as higher risk.
- Lawyers and notary officers should refer to the national risk assessment in the Kingdom; there is a section that presents the risks in the legal sector and assesses sectoral risks, various services are identified, and the inherent risks for each are presented, and any breach of the national risk assessments for services by lawyers and notaries requires a detailed explanation to defend the assessment.
- The service risk is just one element of the client risk assessment and there will be different assessments for client, geography and delivery channel risk that result in the overall client risk assessment. That said the controls applied by the firm may specifically target the service risk e.g. through the way in which certain services are marketed, monitored, contracted for.
- When a Firm decides to have different controls in different parts of the business, it should consider how to deal with clients whose needs straddle departments or functions.
- Before a Firm begins to offer a service significantly different from its existing range of services, it should reperform the assessment of the ML, TF, PF and TFS risks and respond appropriately to any new or increased risks.

Country Risks

- Country risks (or Geographical risks) are represented by the increased level of risk in certain countries concerning services and clients regarding ML/TF/PF
- Factors to consider include whether the country:

  - Has laws that criminalize ML/TF/PF.

  - Has a legislative framework that imposes obligations on financial institutions and DNFBPs regarding CDD, monitoring, STR, and record-keeping similar to those stipulated in the Implementing Regulations.

  - Has an effective and established supervisory system for AML/CFT.
- Countries that have imposed sanctions on individuals or entities due to terrorism or countries that provide funding or sponsorship for terrorism should be considered.
- The state of the rule of law in the country may also be considered, as well as whether a significant portion of its economy operates outside the formal legal system or the infrastructure of legitimate business.
- The results of any recent independent assessment of the country's system in AML/CFT may be considered, such as: The mutual evaluation report issued by the Financial Action Task Force (FATF). These assessments can be found on the websites of the FATF and its regional bodies.
- The controls used for each category must be appropriate to the risks, for example:

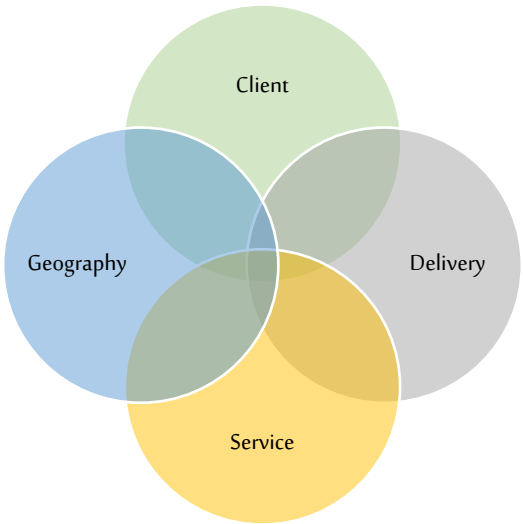
  - If it is common for a law or notarial firm to deal with clients from high-risk countries, the firm's procedures for those considered ordinary clients should be designed to address the risks associated with the high-risk jurisdiction.

  - If the firm has no experience in a particular country, it may treat it as a normal or high risk even if other firms consider it low risk.

  - If a firm expects to deal only with individuals and entities from the Kingdom, it may classify any client or transaction related to a foreign jurisdiction as high risk.

Risks of Service Delivery channels

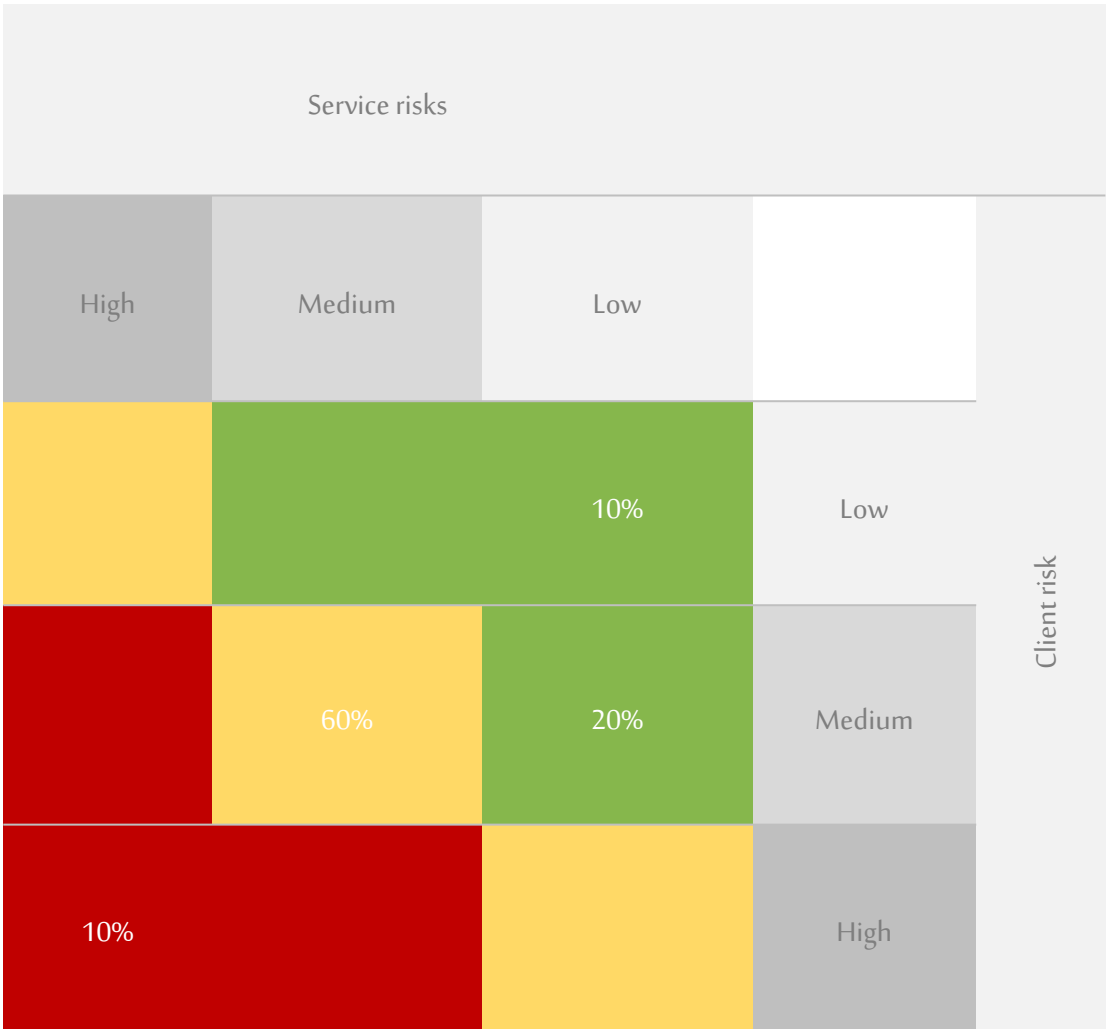
- Certain delivery channels can increase the ML, TF, PF or TFS risk, because they can make it more difficult to perform Client Risk Assessments, CDD or to monitor the relationship.
- For example: delivery channel risk could be increased where services are provided to clients who have not been met face to face, or where a business relationship with a client is conducted through an intermediary. This in turn is affected by the role and degree of control of the intermediary, the location and any restrictions on access to information/data. Where multiple services are provided to a client, the analysis and impact on risk can be recorded as part of delivery channel risk.



Integration and Comparison of Risks

- The various risks may be weighed and should also be considered in combination with each other. Delivery Risk may not be applicable and service risks do not need to be differentiated if the Firm only provides one service.
- The lawyer and notary must be able to demonstrate to the ministry their ability and method of assessment and their efforts to mitigate the risks of ML, TF, and PF, and this assessment must be documented and provided to the ministry upon request, and the documents should clarify how the risk assessment affects the business controls.

- The combination of Client and Service Risk might be illustrated as follows (this assumes an even weighting). In this example, three services are provided: one low, one medium, and one high. When mapped against client risk, we have 30% of the business as low risk, 60% as medium and 10% as high. Resources should be applied more intensely to the high-risk areas, and the controls for the high-risk service enhanced. When identifying the proportion of business, you should apply different or the most appropriate measures, such as: number of clients, number of matters, number of relationships, level of fees, value of transactions.



Thirdly: Due Diligence towards Clients (CDD) and Monitoring

- The purpose of Customer Due Diligence (CDD) is to know and understand a client's identity and business activities so that any ML or TF risks can be properly detected.
- Effective CDD is, therefore, a key element of AML/CFT/CPF/TFS controls. By understanding a client's identity, including who has ultimate ownership and control, a firm not only fulfils its legal and regulatory requirement, but also equips itself to make informed decisions regarding the client's professional standing, acceptability, and overall risk.
- 76. CDD also helps a Firm to construct a better understanding of its typical client profile. By understanding normal practice, it is easier to detect abnormal events, which, in turn, may point to ML or TF/PF.
- Where its services are activities in scope the Firm must ensure that CDD is applied to new and existing clients alike. For existing clients, CDD information gathered previously should be reviewed and updated where it is necessary, timely and risk-appropriate to do so.

Client Risk Assessment

- Each client must be subjected to an assessment of the risks it presents, taking account the client profile, the circumstances including how the client was introduced to You, the service sought, and the geographical elements.
- This must be documented prior to commencing with the transaction, used to determine the level of CDD to be conducted and the ongoing monitoring where applicable, and updated where there are changes, and fed into the aggregate client risk for the Business Risk Assessment for the firm.
- You should maintain a list of clients that can be provided to the MOJ marking each with its respective risk assessment.

- You should keep the assessment within the client file, ensuring that all employees involved with the client are aware but never disclose the assessment to the client. Employees are expected to report to the Compliance Officer where new factors affect the assessment or otherwise, they disagree with the assessment to explain.
- While the Implementing Regulations prescribe the level of CDD that should be applied in certain situations (i.e. simplified or enhanced), they do not describe how to do this on a risk-sensitive basis. The Firm should be able to demonstrate to MOJ that the measures it applied were appropriate. Whilst a Firm may simply adopt High-Medium-Low categories one method to further demonstrate a risk based approach is to consider risk on a scale of 1-10, where:

6 - 10	High risk
EDD procedures	
3 - 5	Medium risk
CDD	
1 - 2	Low risk
SDD	

- CDD should be completed before entering into a business relationship or undertaking a one-off transaction

A "business relationship" means any relationship with a continuing nature, which is established between any of FIs and DNFBPs and its clients related to the activities or services the FIs and DNFBPs provide to them.

- There are of course commercial benefits to having relationships with clients, securing their trust through providing high quality services and in that case the capacity to evaluate the risks and comply with the law in Regulations in relation to the transactions of those clients is enhanced. In that case firms may opt to approach its compliance in respect of relationships which entails an ongoing monitoring requirement and, in every case, to ensure that CDD is appropriate prior to each and every transaction handled for the client. Be clear on your policy in this respect.

Identity verification

- The identification phase requires the gathering of information about a client's identity and the purpose of the intended business relationship. Minimum identification information for an individual is:

  A- Full name.

  B- Date of birth.

  C- Nationality.

  D- Address of residence.

  -E Any other information required by the system.

- This information can be obtained from a range of sources, including the client but exercise caution in higher risk cases. In the case of corporate clients and other legal persons or arrangements, identification also extends to establishing the identity of anyone who ultimately owns or controls the client. These people are the 'beneficial owners' (BOs).

Verification

- Once an initial risk assessment has been carried out, evidence from an independent, reliable source is required to verify the identity information gathered. This is called verification. Whilst the initial risk assessment may highlight a need for more information to be gathered or a fresh risk assessment performed, note that the client risk assessment is continual and will require review especially during verification and monitoring. For this reason, it is not usually effective to take a "tick box" approach to CDD and monitoring.
- Client verification means to verify on the basis of documents or information obtained from a reliable source which is independent of the person whose identity is being verified . Documents issued or made available by an official body can be regarded as being independent of a person even if they are provided or made available by or on behalf of that person.
- Enhanced Due Diligence (EDD) might include more extensive internet and media searches covering the client, key counterparties, the business sectors and jurisdictions. Subscription databases can be a quick way to access this kind of public domain information, and they will often reveal links to Family members and Close Associates of Politically Exposed Persons (PEPS).

Beneficial Ownership

- The Beneficial Owner must be a natural person and cannot be a legal person.
- Whenever you are dealing with a client that is not a natural person, i.e. a legal person (e.g. company) or arrangement.
- If you only have individuals as clients, be aware that people that you deal with, may do so on behalf of another without your knowledge and so you must take steps to be sure that you are dealing with the beneficial owner or identify the BO.
- In many situations determining beneficial ownership is a straightforward matter unless the client is part of a complex structure which may result in a high-risk classification.

Due Diligence for Individuals

Definition	Risks
Full name. - Date of birth. - Address of residence. - Nationality. Any other information required by the system.	All
Verification	Risks
The original, or an acceptably certified copy, of one of the following documents should be seen and a copy retained: Valid passport. - Valid driver's license with photo. - National ID card. - Residence permit (for non-Saudi nationals)	Normal risk CDD
In addition to the above: The original of a second document should be inspected, and a copy retained. It must be one of the following: • A valid full Kingdom of Saudi Arabia driving license. • Recent evidence of entitlement to a state- or local authority-funded benefit • Instrument of a court appointment (such as a liquidator or grant of probate). • Government issued tax notification. • Current bank statements or credit/debit card statements (including electronic if evident issued in that form). • Current utility bill.	High-risk procedures EDD
Source of wealth and source of funds At a minimum search and record from public online information including, company and land registers and depending on risk obtain originals or certified copies of: • Audited financial statements • Bank statements • Proof of property sale • Proof of inheritance • Proof of business sale	

Risk-based due Diligence towards Clients

This is important, not only to ensure that there is good depth of knowledge in higher risk cases, but also to avoid disproportionate effort in lower risk cases.

Risk-based due Diligence towards Clients

- Simplified due diligence (SDD) can be applied in a low-risk case (AML Implementing Regulation 7/14).
- Customer Identification is still required but the extent and timing of verification and the degree of reliance placed on others if applicable, may be adjusted to reflect the assessment of low risk. Ongoing monitoring for unusual or suspicious transactions is still required, and this may be simplified compared to what is done for normal risk, but it is often easier to adopt the same approach to monitoring for both normal and low risk especially given the need to confirm the risk assessment as low.
- The Firm's internal procedures should set out clearly what constitutes reasonable grounds for a client to qualify for SDD and must consider at least the risk factors and this guidance.
- In any case, when a client or potential client has been subjected to SDD, and a suspicion of money laundering or terrorist or proliferation financing arises nonetheless, appropriate (i.e. normal or enhanced) due diligence procedures should be applied instead (with due regard given to any risk of tipping off).

EDD Procedures

EDD procedures may include one or more of the following:

A. seeking additional independent, reliable sources to verify information provided to the Firm;

B. taking additional measures to understand better the background, ownership and financial situation of the client, the beneficial owner and other parties to the transaction;

C. taking further steps to be satisfied that the transaction is consistent with the purpose as stated or the intended nature of the business relationship;

D. Increasing the monitoring of the business relationship or transactions.

PEPS

- PEPS including their family and any associated persons, companies or other legal persons or arrangements ("Close Associates") pose higher ML risks because their positions can make them vulnerable to corruption. It is important to identify PEPs so that the Firm can properly consider the risks associated with any engagement involving them and apply EDD.
- A risk-management system to determine whether a person or BO with whom the Firm has a business relationship is a PEP, a family member, or a close associate should be largely risk-based, particularly in terms of the method of verification and the frequency of screening throughout the relationship. Some Firms may subscribe to commercial databases that record PEPs, their family members, and close associates. Firms that are likely to provide services regularly to PEPs should consider subscribing to such systems. If not, additional information about the client's family and associates may be required so the Firm can verify whether they are PEPs. Identifying close associates of PEPs is particularly difficult without access to a commercial system. Firms should therefore use risk-sensitive measures to assist them in recognizing PEPs. This may be as simple as asking the client directly or conducting online searches.
- During the life of a relationship reasonable steps should be taken to keep abreast of developments that could transform an existing client into a PEP.
- Risk management procedures should include:

1- procedures for requiring that senior management approval be obtained before establishing or continuing a business relationship with a politically exposed person or a family member or close associate;

2- reasonable measures to establish the source of wealth and the source of funds of a person involved in a business relationship and a BO identified as a politically exposed person or a family member or close associate

A- Source of Funds is the source or origin from which funds may be received for fees or if handling transactions, funds.

ب- Source of Wealth is how the person acquired wealth or funds for example employment, property development and other business interests. The earnings from a political career do not usually result in significant wealth. Being in business prior to political career may have generated significant wealth which in many countries should all be disclosed and divested. Extensive checks are required where a client is a PEP to ensure that the funds are not the proceeds of corruption or other illegitimate activity.

3- Monitoring the business relationship with the politically exposed person or a family member or close associate

- In cases where a client (individual) or BO of a client is identified as a PEP, an enhanced level of due diligence must be performed on the PEP. Firms should also undertake an increased level of monitoring in respect of the client relationship, although a risk-based approach may determine what is necessary as PEPs do vary in risk, as does the degree of initial CDD performed and recorded.
- Lawyers and notary officers may determine that an individual is no longer a PEPs after a period has elapsed after they resign from the position. Where PEPs are removed from office Firms should consider the person to be high risk until the reason for removal is made known or proven. This may not apply to family members or known close associates.
- n higher risk cases, however, law and notarial Firms should continue to treat individuals as PEPs after they cease to hold the position and extend the requirements to family members and known close associates of PEPs.

Targeted Financial Sanctions (TFS)

Lawyers and notary officers must comply with any sanctions, embargos or restrictions in respect of any person or state to which the UN, or the Kingdom has decided to apply such measures . Firms may be directed to not enter into business relationships, carry out one-off transactions or proceed with any ongoing arrangements.

Originals and Acceptably Certified Copies for Verification

✓ Certification

- Lawyers and notary officers should consider how they will demonstrate the reliability of document copies.
- In normal or medium risk relationships or transactions, when the original was seen by an employee it should be sufficient for that person to endorse the copy to that effect, including the date on which it was seen, provided they have received training in that regard or are a member of senior management and there should be controls to this effect.
- When the copy originates from outside the Firm, Firms should only accept documents certified by persons who are legally authorized to do so.

✓ Timing and Incomplete CDD

- The AML Implementing Regulations, Article 7 paragraph (3), acknowledge that verification may, in some cases, need to be completed while the business relationship is being established rather than beforehand. However, as noted above, CDD must always be completed before any transactions are executed. In some urgent circumstances, it may be necessary to complete verification while commencing the work. Examples of such cases include:

  A. some insolvency appointments;

  B. appointments that involve ascertaining the client's legal position or defending them in legal proceedings;

  C. response to an urgent cyber incident;

  D. when it is critically important to preserve or extract data or other assets without delay

- When most of the information needed has been collected before the business relationship has begun, it may be acceptable to have a short extension (to allow for information collection to be completed) provided:

a. the cause of the delay is administrative or logistical, not the client's reluctance to cooperate,

b. the reasons are valid and do not give rise to suspicions of money laundering,

c. each extension should be subject to risk-based controls, considered individually and agreed by senior management,

d. extensions should be specific, well-defined and time-limited,

e. there should be no granting of general extensions (such as for client types), and

f. no client assignments (including transfers of client money or assets) should be completed until verification has been completed in accordance with the Firm's procedures.

On-going Monitoring of the Client Relationship

✓ Transactions

Each transaction handled on behalf of a client is a time to ask if it is as expected and commensurate with the client's profile and intended purpose in the relationship. Where legal and notarial Firms treat business only on a transaction-by-transaction basis then On-going monitoring is not typically considered relevant as risk assessments and CDD are required for each transaction.

✓ Trigger-based Monitoring

- Lawyers and notary officers must ensure that the documents, data, and information obtained for CDD purposes are kept up to date. Events that trigger the need to update CDD measures should include the following:

a. a change in the client's identity information

b. a change in beneficial ownership or control of the client

c. a change in the service provided to the client

d. information is obtained that is inconsistent with the Firm' knowledge of the client

e. change in the risk or factors affecting the risk rating

- A review may also be triggered by:

a. the start of a new engagement;

b. planning for recurring engagements;

c. a previously stalled engagement restarting;

d. a significant change to key office holders;

e. the participation of a PEP;

f. a significant change in the client's business activity (this would include new operations in new jurisdictions); and

g. there is knowledge, suspicion or cause for concern (for example, where you doubt the veracity of information provided). If a STR has been made, care must also be taken to avoid making any disclosures which could constitute tipping off).

✓ Periodic Monitoring

- Lawyers and notary officers should also conduct periodic reviews of any relationships to update their CDD. The frequency of updating should be risk-based, reflecting the Firm's knowledge of the client and any changes in its circumstances or the services it requires.

For example:

1-3 years	**Low risk**
6 months to a year	Medium risk
Every month or quarter	High risk

- The CDD procedures required for either Trigger-driven or Periodic reviews may not be the same as when first establishing a new business relationship. Given how much existing information could already be held, on-going CDD may require the collection of less new information than was required at the very outset.

✓ Suspending Operations and Reporting Suspicious Transactions

If a prospective or existing client refuses to provide CDD information, the work must not proceed and any existing relationship with the client must be terminated (AML I Rs 7/8)

Fourth: Reporting Suspicious Transactions (and internal reporting)

- It is an offence for someone who knows or suspects criminal conduct (or has reasonable grounds) to not report their concerns to their MLRO (or to the SAFIU).
- Firms should have internal reporting procedures that enable staff to disclose their knowledge or suspicions of ML or TF and a MLRO should be appointed to receive these disclosures.
- As the types of transactions which may be used by a money launderer are almost unlimited, it is difficult to define a suspicious transaction, but for an established client, a suspicious transaction will often be one which is inconsistent with that client's known, legitimate business or personal activities. Therefore, the first key to recognition is knowing enough about the client and the client's business to recognize that a transaction, or series of transactions, is unusual. Such transactions may arise at any stage and commonly occur within an established relationship rather than at the outset or as part of a one-off transaction.
- Warning signs which can indicate that an established client's transaction might be suspicious include:

a. the size of the transaction (or transactions when aggregated) is inconsistent with the normal activities of the client;

b. the transaction is not rational in the context of the client's business or personal activities;

c. the pattern of transactions conducted by the client has changed;

d. the client has no obvious reason for conducting business with a country involved in the transaction.

- The type of situations giving rise to suspicion will depend on a firm's client base and range of services. Sufficient direction must be given to partners and staff to enable them to recognize suspicious transactions. Firms might also consider monitoring the types of transactions and circumstances that have given rise to STRs, with a view to updating internal controls from time to time.

- Reporting lines should be as short as possible, with the minimum number of people between the person with suspicion and the MLRO. This ensures speed, confidentiality and accessibility to MLRO.
- Partners should be aware of their own legal obligations and should never attempt to prevent a member of staff who remains suspicious from reporting directly to the MLRO. Staff should be made aware that they have a direct route to the MLRO.
- All procedures and responsibilities should be documented in appropriate manuals and job descriptions where necessary.
- All suspicions reported to the MLRO should be documented. In some legal and notarial firms it may be possible for the person with the suspicion to discuss it with the MLRO and for the report to be prepared jointly. In other firms the initial report should be prepared and sent to the MLRO. The report should include full details of the client and as full a statement as possible of the information giving rise to the suspicion.

Fifth: Record Keeping

- Records relating to CDD, including non-engagement documents relating to client relationships, any transactions and correspondence must be kept for at least (10) years from the end of the client relationship. A disengagement letter is documentary evidence that a business relationship has terminated, but other forms of communication such as emails may suffice.
- All records related to a one-off transaction must be retained for (10) years after the date of the transaction.
- The Implementing Regulations do not specify the form in which records should be kept, but they must be readily retrievable

- There is no formal retention period specified for records related to:
  a. internal reports;
  b. the MLRO's consideration of internal reports;
  c. any subsequent reporting decisions;
  d. issues connected to consent, production of documents and similar matters;
  e. suspicious activity reports and consent requests sent to the SAFIU, or its responses.
- However, since these records can form the basis of a defense against accusations of ML and related offences, lawyers and notary officers should determine and apply a suitable retention period.
- Records related to internal and external reports of suspicious activity are not part of the working papers relating to client assignments. They should be stored separately and securely as a safeguard against tipping off and inadvertent disclosure to someone making routine use of client working papers.
- Legal and notarial firms must demonstrate their compliance with Implementing Regulations that place a legal obligation on them to make sure that some of their employees are:

  (a) aware of the law relating to ML, TF, and PF (b) trained regularly in how to recognize and deal with transactions and other events which may be related to ML or TF.

  Records should show the training that was given, the dates on which it was given, which individuals received the training and the results from any assessments.

Training and Awareness

- The AML and CFT Implementing Regulations require that all employees are given ongoing training. This should include:

a. AML/CTF/CPF and TFS laws;
b. the Firm's policies and procedures; and
c. how to recognize and deal with transactions which may be related to ML/TF/PF and TFS, as well as to identify and report anything that gives grounds for suspicion.

- A formal training plan can help make sure that the right staff receive the right training to enable them to comply with their obligations but if in doubt basic training should be provided for all staff.
- Lawyers and notary officers must must participate effectively in the training programs and workshops provided or announced by the Ministry, and must convey the knowledge gained to the employees within their Firms..

What should Training Include?

- Training can be delivered in several different ways: face-to-face, self-study, e-learning, video presentations, or a combination of all of them The key is to ensure engagement by staff as to the importance of the training.
- The program itself should include:

أ- An explanation of the law within the context of the firm's own commercial activities.

ب- The Firm's policies and procedures. How to deal with transactions that might be related to ML/TF/PF/TFS (including how to use internal reporting controls), the firm's expectations of confidentiality, and how to avoid tipping off.

- Where applicable, training programs should be tailored to each business area and cover the firm's procedures so that staff members understand the ML/TF/PF/TFS risks posed by the specific services they provide and types of client that they deal with. Furthermore, legal and notarial firms should aim to create a culture in which staff are always alert to the ML/TF/PF/TFS risks and habitually adopt a RBA to CDD.
- A system of tests, or some other way of confirming the effectiveness of the training, should be conducted, either separately or as part of the employees' performance appraisal.

When should Training be Completed?

- Firms must ensure that new employees are trained promptly. Where delays occur, appropriate controls must be applied to mitigate any risks arising from the lack of training.
- Firms must reflect changes in laws, Implementing Regulations, professional standards, and judicial findings (whether domestic or international), as well as changes in the risk profile and operating procedures, in the frequency of their training programs.
- Otherwise, it may not be necessary to repeat a complete training program annually, but it may be appropriate to provide employees with concise updates to help refresh and expand their knowledge and to remind them of the importance of effective AML, CTF, CPF and TFS controls. There are always matters and topics that related to AML, CTF, CPF and TFS to provide training on.
- In addition to training, Firms are encouraged to run periodic AML, CTF,CPF awareness campaigns to keep staff alert to individual and firm-wide responsibilities


رؤية VISION
2030
المملكة العربية السعودية
KINGDOM OF SAUDI ARABIA
وزارة العدل
MINISTRY OF JUSTICE