Talal Abu-Ghazaleh Global

TAG.Global

The International Arab Society of Certified Accountants (IASCA)

Member of TAG-Foundation

ANTI- MONEY LAUNDERING & COUNTER FINANCING OF TERRORISM

Guidelines for the Accountants in the Arab Region

Amman - Jordan - 2022

Anti-Money Laundering and Counter-Financing of Terrorism

Guidelines for the Accountants in the Arab Region

This handbook was jointly prepared by TAG.Global and the International Arab Society of Certified Accountants (IASCA). All reasonable care has been taken in the preparation of these Guidelines, but it necessarily contains concise information and is therefore intended for general guidance only. The publication does not amend or override, and it is not intended to be a substitute for reading the Laws, Regulations and guidance issued in each Arab country as well as by the United Nations.

A person should utilize his/her professional judgment and the facts and circumstances involved in each particular case. The information presented in the Guidelines should not be construed as legal, auditing, or any other professional advice or service. After reading these Guidelines, if you do not fully understand your obligations, you should seek legal advice or contact your AML/CFT supervisor.

Disclaimer: TAG-Gobal and IASCA do not accept any liability to any party for any loss, damage or costs whatsoever arising from any action or decision taken, or not taken, as a result of relying on this publication, whether the loss is due to negligence or otherwise.

The approved text of the Anti-Money Laundering and Terrorist Financing Handbook is the text prepared jointly by (TAG.Global) and (IASCA) in Arabic, and it has been translated into English.

Original title: Anti Money Laundering and Counter Financing of Terrorism 2023 Edition, ISBN:978-9957-8696-9-4

The handbook is available for free download on the website.
https://www.iascasociety.org / https://www.tagorg.com
Deposit number at the National Library Department: 423/1/2023
ISBN: 978-9957-8696-9-4

---

kindly send the publications and issues related to copyrights to: -

TAG.Global
طلال أبو غزالة العالمية
Talal Abu-Ghazaleh Global
quality.control@tagi.com

info@iascasociety.org

Amman - The Hashemite Kingdom of Jordan

The Hashemite Kingdom of Jordan
The Deposit Number at the National Library
2023/1/425

345.5650231
The International Arab Society of Certified Accountants
Anti-Money Laundering and Counter Financing of Terrorism/ The International Arab Society of Certified Accountants, Talal Abu-Ghazaleh Organization.- Amman: Prepares,2023

() p.
Deposit Number: 2023/1/425
Descriptors: /Obligations (Law)//Accountants/ Money/ Laundering//Terrorism//Criminal Law.

Introduction

Money Laundering (ML) is the practice of "legitimizing" the proceeds of crime by filtering them into the regular economy to disguise their illegal origin. The Financial Action Task Force (FATF) defines "Money Laundering" as the processing of criminal proceeds to disguise their illegal origin in order to legitimize the ill-gotten gains of crime.

There are no accurate statistics identifying the amount of money laundered worldwide. A commonly referenced estimate is about 2-5% of global GDP, or $800 billion - $2 trillion in current US dollar, which was produced by the UN Office on Drugs and Crime (UNODC) in 2021.

Money laundering was essentially limited to financial institutions by abusing the financial and banking sectors to conceal and disguise the criminal nature of some funds. However, this phenomenon expanded to include designated non-financial businesses and professions (DNFBPs) (including legal professions such as accountants, lawyers, trust, and company service providers) to be used for the same purpose. This prompted the FATF, in 2003, to extend its recommendations on combating money laundering and the financing of terrorism, to certain Non-Financial Businesses and Professions, and to set out the submission of the DNFBPs to Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) requirements. This draw-up or expansion was not general, but rather limited to some activities conducted by such professions, which involve ML/TF risks.

Risks associated with accountants, as independent professionals, in the ML/TF field, lie basically in the potential use of this profession to conceal the identity of the beneficial owners, engage in financial transactions, or provide services that may help disguise the proceeds of the criminal activities in order to conceal their illicit source.

In general, due to their high risks, countries have criminalized ML and TF and imposed penalties against the perpetrators. However, in order to comprehensively address money laundering, a preventive approach, along with a dissuasive or penal approach must be adopted. Financial institutions and designated non-financial businesses and professions (DNFBPs, including accountants) will have obligations and responsibilities to abide by in order to prevent or detect ML or TF operations or identify perpetrators. The AML/CFT regime requires the integration of both the preventive and dissuasive approaches.

Although Arab States have included accountants in their AML/CFT systems in response to recommendations made by the FATF, up-to-date AML/CFT guidelines for accountants in the Arab region as a whole, are still needed.

To prepare these guidelines, many similar AML/CFT guidelines for accountants, in different regions, unions, and developed as well as developing countries in various continents, were reviewed.

The main purpose of the Anti-Money Laundering and Counter Financing of Terrorism (AML / CFT) - Guidelines for Accountants ("The Guidelines") is to provide guidance for accountants providing specified services subject to AML/CFT legislations in the Arab region.

These guidelines have included all concepts and procedures that accountants must know, to enable them to combat money laundering and terrorist financing, of which; the definition of money laundering and terrorist financing, how to implement the risk-based approach (RBA), how to do Customer Due Diligence (CDD), how to Report Suspicious Activities (RSA), to whom should accountants report, how to keep records and do training and awareness.

These guidelines follow the broad outline of the FATF guidance for a Risk-Based Approach for Accounting Profession and fulfil the requirements of the FATF 40 recommendations on accountancy obligations regarding AML/CFT compliance requirements, and adopt the most recent and advanced guidelines applied in developed countries.

These guidelines are intended to be read by anyone who provides audit, accountancy, tax advisory, insolvency, or trust and company services in the Arab region, and have been approved, adopted and will always be updated by the International Arab Society of Certified Accountants (IASCA).

These guidelines set out the responsibilities of the accountant in combating money laundering, which include: developing and maintaining a risk assessment framework; ensuring that adequate AML policies are put in place, kept up to date and implemented effectively on an ongoing basis; advising senior management before a final decision is taken on engaging new high-risk customers; monitoring AML policies and procedures for compliance with obligations; advising the management body on measures to be taken; producing an annual activity report; reporting suspicious transactions to the national Financial Intelligence Unit; and overseeing internal AML training and awareness raising.

Accountants are key gatekeepers for the financial system, facilitating vital transactions that underpin the economy. As such, they have a significant role to play in ensuring their services are not used to further a criminal purpose. As professionals, accountants must act with integrity and uphold the law, and they must not engage in criminal activity. For both accountancy firms and sole practitioners, failing to comply with AML regulations can have severe consequences; these range from fines to court proceedings or even a prison sentence in certain countries.

The reason accountants are subject to the FATF standards and AML / CFT measures is because accountants are "gatekeepers" to the financial system. Arising from the financial and consultancy nature of work, accountants may have a higher chance of crossing paths with money launderers or dealing with illicit funds from ML or TF. Money launderers or terrorism financiers may obtain assistance from accountants without them fully realizing it. In other words, the expertise of qualified accountants can be used to disguise illegal transactions, and make them appear legitimate – this is why the accountancy sector is often targeted by those who carry out financial crime.

There are three key tell-tale signs which accountants should look out for when trying to prevent money laundering. These are as follows: (1) If a long-term client or customer behaves oddly, or makes uncharacteristic requests. (2) A client or customer asks you to make financial arrangements, which do not make sense commercially. (3) A client or customer asks you to provide services, which are outside your area of expertise and does so on multiple occasions.

In consideration of their role in the business world, it is recognized that accounting firms (ranging from a sole practitioner to a large firm), and their staff can contribute to AML/CFT. Accordingly, it is crucial for firms and their staff to be familiar with the risks and crime of ML and TF, and their role to report actual and suspected ML and TF activities. There is also a role on countering proliferation financing (CPF), but this is limited to targeted financial sanctions under the AML/CFT legislation.

We encourage accountants and other professionals to develop an understanding of the ML/TF risks in the wider sectors and industries that they have business dealings with as well. Given these risks, and the FATF recommendations, governments have chosen to engage gatekeeper professions in the collective efforts to deter and detect these crimes. The more eyes and ears attuned to the indicators (or red flags) of these crime types, the more likely people will struggle to benefit financially from criminal activities. By expanding the AML/CFT system to include the gatekeeper professions, governments intend that gatekeepers will be better able to protect themselves from customers who launder money and finance terrorism. We also recommend that countries develop their own checklists to help accountants comply with both local and international AML/CFT rules and regulations. The most important of which are; a checklist to help accountants evaluate the risks related to their sectors, clients, and jurisdictions in which they operate, as well as a checklist to help accountants apply CDD properly.

This guidance has been approved by the International Arab Society of Certified Accountants (IASCA). Therefore, its contents can help accountants comply with their obligations under the Arab States Anti-Money Laundering and Counter-

Terrorism Financing (AML & CTF) laws and legislations, and the FATF regulations and guidelines on AML/CFT, to prevent, recognize and report money laundering. However, courts should refer to the local laws and regulations as well as international regulations to help them decide whether a business subject to these laws and regulations has committed an offence or not.

I am incredibly grateful for the support we obtained from a group of high professionals, who contributed to launching this handbook. Dr. Adly Qandah, an expert in economic and financial advisor, for his ongoing support; Mr. Hazim Farah, quality control manager atTAG-global, for revising the handbook, and Mr. Salem Al Ouri, IASCA's executive director, for his efforts in attaining this achievement.

Talal Abu-Ghazaleh

Dr. Talal Abu-Ghazaleh

HE Dr. Talal Abu-Ghazaleh, born on April 22, 1938, in Jaffa, is the Chairman and Founder of Talal Abu-Ghazaleh Global (TAG.Global). Founded in 1972. TAG.Global is an international professional services organization, which operates out of more than 100 offices in the Middle East, North Africa, Pakistan, India, Cyprus and China. It has representative offices in Europe and North America and non-exclusive strategic alliance agreements with various networks and individual firms, lifetime achievements, distinctions and outstanding contributions to education, accountancy, Intellectual Property, business administration and management, commerce, ICT, science and technology.

Dr. Abu-Ghazaleh is also the chairman and founder of the International Arab Society of Certified Accountants (IASCA), which was established on January 12, 1984, as a non-profit professional accounting association in London, UK. It was formally registered in Amman on February 24, 1994, under the name “The International Arab Society of Certified Accountants (ASCA)”.

IASCA became the destination for the graduates of accounting, commerce, and economy as well as the Arab practitioner accountants to gain knowledge and enhance their academic and professional capacities, to seek advanced qualification by being awarded with IASCA's certificates, which qualify them to practice the profession in many countries.

Moreover, IASCA's certificates are academically and internationally recognized based on the level of curricula, scientific review, examination administration, and the accomplishment of IASCA over the past 30 years by establishing the standards to monitor the performance of accountants and members of professional societies and organizations who are members of the International Federation of Accountants (IFAC) to ensure the performance and commitment to the relevant international standards and practices.

IASCA played vital role and exclusivity as it is the only Arab body entrusted with the translation of the publications, IFAC, and John Wiely and Sons® such as ISAs, IPSASs, as well as printing, publishing and distributing the International Financial Reporting Standards (IFRS) and IFRS for SMEs.

Table of Contents

In a Nutshell

(1) How to know if you are captured by the AML/CFT Act

Box (1) below provides a quick way to check if you are captured under the AML/CFT Act.

Am I captured by the AML/CFT Act as a Designated Non-Financial Business and Profession DNFBP?

Figure (1)

Are you an accounting practice?

YES

Do you do any of the following activities in the ordinary course of business?

Buy and sell of real estate, or commercial stores;

OR

Manage client money, securities, or other assets;

OR

Manage bank accounts, postal savings, investments, or securities accounts in local and international financial markets;

OR

Organize contributions to the creation, operation, or management of companies;

OR

create, operate or manage legal persons or arrangements, and buy and sell business entities

YES

You are captured and must comply with the AML/CFT Act

(2) What Do You Need to Do to Comply?

Step 1: Establish a Compliance Program

Appoint a compliance officer

Reporting entities must appoint a compliance officer who will have responsibility for administering and maintaining the AML/CFT program. An employee should be appointed to this role who reports to a senior manager. In the case of a sole practitioner, we would expect the sole practitioner to be the compliance officer. If that is not possible, an external person must be appointed as a compliance officer.

Conduct a risk assessment

Reporting entities are required to undertake an assessment of the risks posed to their business by money laundering and financing of terrorism crimes. The risk assessment should be in writing and have regard to the applicable guidance material.

Develop an AML/CFT program

The AML/CFT program must be based on the risk assessment described above and be in writing. It should include procedures, policies and controls for ensuring all compliance obligations are adequately and effectively met and must have regard to the applicable guidance material.

Step 2: Maintain your compliance program

Conduct Customer Due Diligence (CDD)

Reporting entities must conduct CDD when conducting an occasional transaction or activity or when establishing a business relationship with a client who is requesting assistance with a captured activity, or when an existing client makes this kind of request (if the reporting entity doesn't hold all the information required already). There are three levels of CDD depending on the circumstances.

Keep records

Reporting entities must keep records of transactions, suspicious activities, documents verifying the identities of customers and other parties or beneficiaries, and any other related records that may be of interest to the supervisor. Records must be kept for at least five years.

Ongoing Customer Due Diligence (CDD) and ongoing account monitoring

Reporting entities are required to undertake ongoing CDD and ongoing account monitoring. This is to ensure that you have ongoing confidence that the business relationship and the transactions within the relationship are consistent with the customer's business and risk profile, and you can spot any suspicious activity early.

Review your compliance program

The supervisor expects reporting entities to conduct a regular review of their compliance program. This is to ensure that any business changes or new risks in the operating environment are referenced in the program and remain fit for purpose.

Step 3: Report and audit

Submit an annual report

Reporting entities must submit an annual report. This report must be in the prescribed form and be submitted to the supervisor at the time set by the supervisor. The report must take into account the results and implications of the audit and any information prescribed in the regulations.

Audit your risk assessment and compliance program periodically

A reporting entity must regularly review its risk assessment and compliance program and have it audited by an independent person who is suitably qualified to conduct the audit. Supervisors may also require an audit to be undertaken on request at shorter notice.

Report to the Financial Intelligence Unit (FIU)

When reporting entities identify suspicious activity, they must report it to the FIU. They should also submit prescribed transaction reports to the FIU as necessary.

SECTION (I)

ABOUT THIS GUIDANCE

1. What is the purpose of this guidance?

This guidance has been prepared to:

- Help accountants (including tax advisers and insolvency practitioners) comply with their obligations under the Arab States Anti-Money Laundering and Counter-Terrorism Financing (AML & CTF) laws and legislations, and the FATF regulations and guidelines on AML/CFT, to prevent, recognize and report money laundering. Compliance with it will ensure compliance with the relevant legislation and professional requirements.
- Support a common understanding of a RBA for the accountancy profession, financial institutions, and designated non-financial businesses and professions (DNFPBs) that maintain relationships with accountants, competent authorities, and self-regulatory bodies (SRBs) responsible for monitoring the compliance of accountants with their AML/CFT obligations;
- Assist Arab countries, competent authorities, and accountants in the design and implementation of a RBA to AML/CFT by providing guidelines and examples of current practice, with a particular focus on providing advice to sole practitioners and small firms;
- Recognize the difference in the RBA for different accountants providing diverse services such as statutory audit, financial and tax advice, and insolvency-related services, among others;
- Outline the key elements involved in applying a RBA to AML/CFT related to accountants;
- Highlight that financial institutions that have accountants as clients should identify, assess and manage the ML/TF risk associated with accountants and their services;
- Assist Arab countries, competent authorities, and SRBs in the implementation of the FATF Recommendations with respect to accountants, particularly Recommendations 22, 23, and 28; and
- Support the effective implementation and supervision of national AML/CFT measures, by focusing on risks as well as preventive and mitigating measures.

2. Why are accountants required to comply with AML/CFT?

The reason, accountants are subject to the FATF standards and AML / CFT measures, is because accountants are “gatekeepers” to the financial system. Arising from the financial and consultancy nature of work, accountants may have a higher chance of crossing paths with money launderers or dealing with illicit funds from Money Laundering (ML) or Terrorism Financing (TF). Money launderers or terrorism financiers may obtain assistance from accountants without them fully realizing it.

In consideration of their role in the business world, it is recognized that accounting firms (ranging from a sole practitioner to a large firm), and their staff can contribute to AML / CFT. Accordingly, it is crucial for firms and their staff to be familiar with the risks and crime of ML and TF, and their role to report actual and suspected ML and TF activities. There is also a role on Countering Proliferation Financing (CPF), but this is limited to targeted financial sanctions under the AML / CFT legislation.

3. What is the legal status of this guidance?

This guidance has been approved by the International Arab Society of Certified Accountants (IASCA). Therefore, its contents can help accountants, as mentioned in point (1) above, comply with their obligations under the Arab States Anti-Money Laundering and Counter-Terrorism Financing (AML & CTF) laws and legislations, and the FATF regulations and guidelines on AML/CFT, to prevent, recognize and report money laundering. However, courts should refer to the local laws and regulations as well as international regulations to help them decide whether a business subject to these laws and regulations has committed an offence or not. This guidance is not intended to be exhaustive. If in doubt, seek appropriate advice or consult your anti-money laundering supervisory authority. If anti-money laundering supervisory authority is called upon to judge whether a business has complied with its general ethical or regulatory requirements, it is likely to be influenced by whether or not the business has applied the provisions of the related national and international AML/CFT laws and regulations.

SECTION (II)

BACKGROUND

This section provides information about:-

1. Financial Action Task Force (FATF)

The FATF is an international task force established in 1989 to develop international standards to combat ML, TF, and the Financing of Proliferation (PF). FATF is the world's Anti–Money Laundering (AML) watchdog. The FATF published a revised set of 40 Recommendations on AML / CFT measures in 2012, which are being continuously updated. Further information on the FATF is available at: http://www.fatf-gafi.org/

2. FATF 40 Recommendations

The FATF 40 Recommendations (along with their Interpretive Notes and Glossary) provide a complete set of counter-measures against ML and TF covering the criminal justice system and law enforcement, preventive measures in the financial and Designated Non-Financial Businesses and Professions (DNFBPs), and international cooperation.

The Arab States have included accountants in the AML/CFT system in response to recommendations made by the FATF.

The FATF Recommendations of specific concerns to accountants are those covering DNFBPs. DNFBPs include the following:-

- Casinos
- Real estate agents
- Dealers in precious metals and stones
- Trust and company service providers
- Lawyers, notaries, other independent legal professionals, and accountants – when they prepare for or carry out transactions for their customers concerning the following activities:
  - Buying and selling of real estate, or commercial stores;
  - Managing of client money, securities, or other assets;
  - Management of bank accounts, postal savings, investments, or securities accounts in local and international financial markets;
  - Organization of contributions to the creation, operation, or management of companies;
  - Creation, operation, or management of legal persons or arrangements, and buying and selling of business entities.

The applicable FATF Recommendations for accountants (and other DNFBPs) are:

- FATF Recommendation 22 (DNFBPs: Customer due diligence)
- FATF Recommendation 23 (DNFBPs: Other measures)
- FATF Recommendation 28 (Regulation and supervision of DNFBPs)

Other FATF Recommendations, which are not specifically targeted at DNFBPs, but are also applicable to DNFBPs include:-

- FATF Recommendation 1 (Assessing risks & applying a risk-based approach)
- FATF Recommendation 6 (Targeted financial sanctions related to terrorism & TF)
- FATF Recommendation 7 (Targeted financial sanctions related to PF)
- FATF Recommendation 35 (Sanctions)

Further information on the FATF Recommendations is available at: https://www.fatf-gafi.org/publications/fatfrecommendations/?hf=10&b=0&s=desc(fatf_releasedate)

3. Middle East & North Africa Financial Action Task Force (MENA-FATF)

The Governments of 14 Arab States decided, on November 30, 2004, to establish MENAFATF as a FATF Style Regional Body (FSRB), at an inaugural Ministerial Meeting held in Manama, Bahrain. It was agreed that the headquarters of this body will be in the Kingdom of Bahrain.

The MENAFATF is voluntary and cooperative in nature and independent from any other international body or organization; it was established by agreement between the governments of its members and is not based on an international treaty. It sets its own work, regulations, rules, and procedures and cooperates with other international bodies, notably the FATF, to achieve its objectives. Further information on the MENAFATF is available at: https://www.menafatf.org/

4. Money Laundering

Money laundering is the practice of "legitimizing" the proceeds of crime by filtering them into the regular economy to disguise their illegal origin. The FATF defines "Money Laundering" as the processing of criminal proceeds to disguise their illegal origin in order to legitimize the ill-gotten gains of crime.

There are no accurate statistics identifying the amount of money laundered worldwide. A commonly referenced estimate is about 2 - 5% of global GDP, or $800 billion - $2 trillion in current US dollar, which was produced by the UN Office on Drugs and Crime in 2021. It is difficult to estimate the scale of money laundering because, by its very nature, the activity is not disclosed unless detected. However, it is increasingly global, with criminals often seeking to launder money where controls are the weakest, often far from the source of the funds. Due to the clandestine nature of money laundering, it is, however, difficult to estimate the total amount of money that goes through the laundering cycle. Within Europe, Europol estimates the value of suspicious transactions in the hundreds of billions of Euros – at an equivalent of 1.3% of the EU's gross domestic product (GDP) in 2021.

Money laundering can be traced through a series of stages. The initial stage is placement, where illegal proceeds are introduced to the financial system, often broken up into smaller amounts. The second stage is layering, where the funds are moved around or converted to disguise their source. Finally, integration describes the stage in which criminals spend or invest the laundered proceeds in the legitimate economy. Money laundering can occur right across the economy, from gambling to commodity trades and property purchases. However, at some stage launderers usually need to use the banking system, particularly when layering illegal proceeds. The most recent Eurostat figures showed that over 75% of suspicious transactions reported in the EU were disclosed by credit institutions in more than half of the Member States. A threat related to money laundering is terrorism financing, which involves the supply of funds to terrorist organizations, very often across international borders. In some ways, terrorism financing is the reverse of money laundering, as quite often small sums of legitimate proceeds are pooled and put to use for terrorist activity. Since both activities involve illegal financial flows, however, they are generally dealt with under the same legislative and security headings.

The goal of a large number of criminal acts is to generate a profit for the individual or group that carries out the act. Money laundering is the processing of these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardizing their source.

Illegal arms sales, smuggling, and the activities of organized crime, including for example drug trafficking and prostitution rings, can generate huge amounts of proceeds. Embezzlement, insider trading, bribery, and computer fraud schemes can also produce large profits and create the incentive to “legitimize” the ill-gotten gains through money laundering.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention.

Criminal property may take any form, including:-

- Money or money’s worth;
- Securities;
- A reduction in a liability; and
- Tangible or intangible property.

Money laundering can involve the proceeds of offending in the Arab States but also of conduct overseas that would have been an offence had it taken place in the Arab countries. There is no need for the proceeds to pass through the Arab countries. For the purposes of this guidance money laundering also includes terrorism financing. There are no materiality or de minimis exceptions to Money Laundering or Terrorism Financing (MLTF) offences.

Money laundering activity can include:-

- A single act (for example, possessing the proceeds of one's own crime);
- Complex and sophisticated schemes involving multiple parties;
- Multiple methods of handling and transferring criminal property; or
- Concealing criminal property or entering into arrangements to assist others to conceal criminal property.

Businesses need to be alert to the risks posed by:-

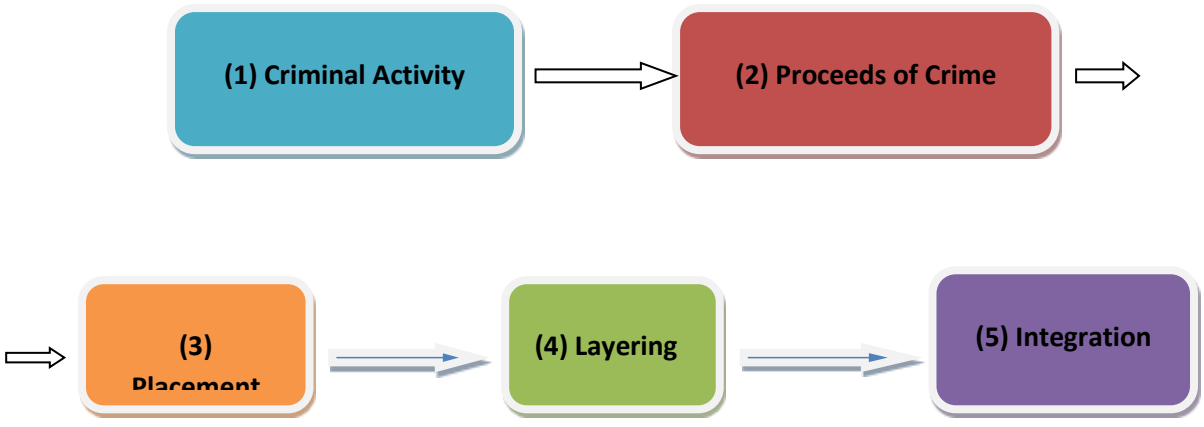
- Clients;
- Suppliers;
- Employees; and
- The customers, suppliers, employees, and associates of clients.

Neither the business nor its client needs to have been party to money laundering for a reporting obligation to arise.

5. HOW MONEY LAUNDERING WORKS

Money laundering works by taking proceeds of illegal (criminal) activity and disassociating them from the underlying crime by placement, layering, and integration into the legitimate financial system.

Figure 2: How Money Laundering Takes Place



5.1 CRIMINAL ACTIVITY

This includes illegal arms sales, smuggling, and organized crime, including for example drug trafficking and prostitution, embezzlement, insider trading, bribery, and computer fraud schemes.

5.2 PROCEEDS OF CRIME

The illegal origin of the criminal proceeds can take the form of financial instruments such as cash into less conspicuous smaller sums, or by using other monetary instruments (cheques, wire transfers, money orders, etc.)

5.3 PLACEMENT

The launderer introduces the illegal profits into the financial system. This might be done by breaking up large amounts of cash into less conspicuous smaller sums that are then deposited directly into a bank account, or by purchasing a series of monetary instruments (cheques, money orders, etc.) that are then collected and deposited into accounts at another location. Possible methods include:

- Change currency & denomination
- Transport cash
- Cash deposits

5.4 LAYERING

The launderer engages in a series of conversions or movements of the funds to distance them from their source. The funds might be channelled through the purchase and sale of investment instruments, or the launderer might simply wire the funds through a series of accounts at various banks across the globe. This use of widely scattered accounts for laundering is especially prevalent in those jurisdictions that do not cooperate in anti-money laundering investigations. In some instances, the launderer might disguise the transfers as payments for goods or services, thus giving them a legitimate appearance. Possible methods include:

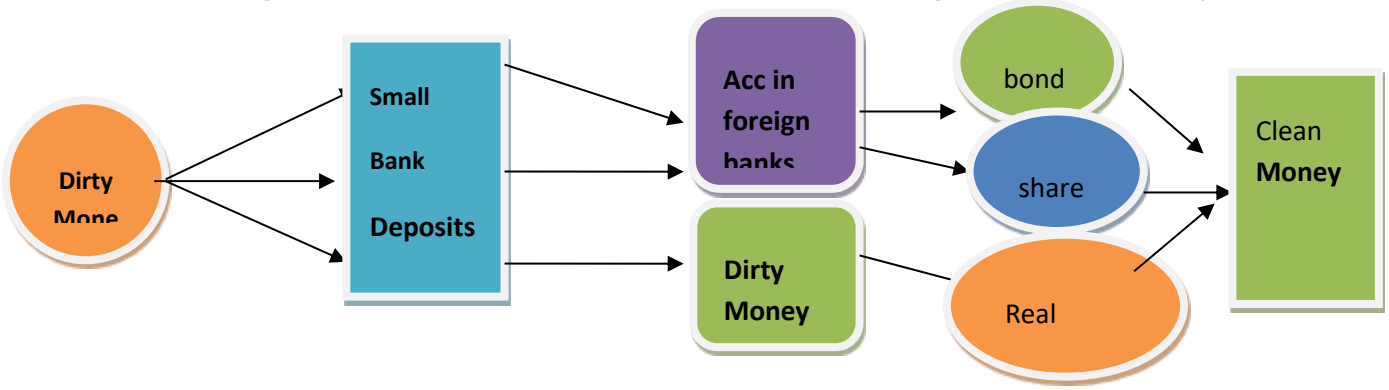
- Wire Transfers
- Withdraw Cash
- Split and Merge Accounts

5.5 INTEGRATION

As illustrated in Figure (3) below, the illicit funds re-enter the legitimate economy. The funds may be invested in real estate, luxury goods, and businesses. Possible methods include:

- Fictitious loans/turnover/contracts
- Disguise ownership of assets
- Use in third-party transactions

Figure (3) How Illicit Funds Re-enter the Legitimate Economy



6. Methods of Money Laundering

The methods and mechanisms of Money Laundering (ML) are diverse and multiple. The following are the most significant ML methods:

- **Structuring or Smurfing**: Cash amounts are structured and broken up into smaller amounts and deposited in financial institutions to be layered below the applicable designated threshold of reporting. This method requires the use of "mules" that are often trusted by, or close associates of, the launderer.
- **Purchase of Assets in Cash**: Launderers aim at purchasing high-value assets in cash, such as cars, yachts, gold, or jewellery. Afterwards, **launderers** use or sell these assets but often register them in the names of close associates to avoid raising doubts.
- **Smuggling of Significant Cash Amounts**: Significant amounts of cash are smuggled across borders to another State and **deposited** in an offshore bank having strict rules in terms of bank secrecy and without an effective AML/CFT regime.
- **Cash-intensive Businesses**: Money launderers usually engage in cash revenue-producing activities and businesses. The accounts of such activities and businesses are then used to deposit **funds** generated from a criminal activity. These businesses operate openly and thus generate cash proceeds from legitimate activities (conducted secondarily), in addition to illicit cash. In such cases, these businesses usually pretend that all cash received is legitimate profits from their apparent activities (cash-intensive activities), and these activities are mostly related to the services sector given the difficulty in discovering the differences between revenues and costs, such as restaurants, bars, casinos, parking, etc.
- **Trade-based Money Laundering**: It is the process of disguising the proceeds of crime and moving (or manipulating) value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity, or quality of imports or exports. Moreover, trade-based money laundering

techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail. For example, artworks can be used for money laundering purposes, given that their price is related to many subjective factors as well as the absolute confidentiality of the persons involved in this sector in terms of not disclosing the identity of the buyer and seller.

- **Alteration of Value**: The launderer purchases a property from a person willing to become an accomplice, by stating in the Contract of Sale a value for the property less than its actual price. For example, the launderer purchases a property that is worth US$ 1 million, but in the Contract of Sale, the value is stated US$ 500, 000 only. After a short period of time, the property is sold at its actual price (i.e. US$ 1 million), and the launderer obtains false justification of the source of the funds at about US$ 500,000.
- **Money Laundering Through Life Insurance Contracts**: The launderer enters into a life insurance contract at high premiums, then cancels or renounces the contract and receives a part of the amount agreed upon; to receive later on a justification for the funds obtained illicitly.

The above methods reflect the general money laundering patterns. However, some other methods involve DNFBPs (specifically legal professions and accountants) in terms of planning and implementing ML schemes. The FATF considers that professionals, practitioners, and experts may largely contribute to the enhancement of the capacities of perpetrators by planning complex and advanced ML schemes to conceal, collect, move or use illicit sources of wealth; including but not limited to:

- **Establishing Shell Trusts**: Trusts may be used to conceal or obscure the beneficial owners of funds, by **separating** the legal ownership from the beneficial ownership (or the effective control) of the assets.
- **Self-borrowing Schemes:** Whereas launderers lend themselves their own laundered proceeds, the launderer hands over the illicit funds to an accomplice, who lends back the launderer an amount equal to the amount previously received from him. This transaction is then documented in a loan contract (in good and due form) to legitimize the funds of the launderers.
- **Establishing Shell Companies**: These are incorporated companies (legal entities), but have no independent operations, significant assets, ongoing business activities, or employees. Shell companies are often established with several forms of ownership structures, with the participation of partners from several countries.

- **Designing and Conception of Schemes**: Aimed at concealing the beneficial owner of a legal person, in order to allow the **separation** between the natural person (money launderer) and the funds derived from a criminal offence.
- **Establishing and Managing Front Companies**: A front company is a fully functioning company with the characteristics of a legitimate business. Front companies often operate in service-oriented businesses such as restaurants, clubs and salons; as such businesses are cash-intensive. Front companies are used in money laundering by integrating and mixing the criminal proceeds with the proceeds of legitimate activities of the said companies.
- **Concealing the Beneficial Owner of Natural Persons**: This allows separation between the natural person (launderer) and funds generated from criminal activities, such as designing a complex ownership and control structure of overlapping layers of partners of legal **persons**, to conceal and separate between the beneficial owners and assets, multiple beneficiaries of one account, and use of legal persons such as directors or board members.
- **Serving as Nominee Directors for Some Companies**: While deliberately not disclosing the nominator or actual and real director.
- **Providing Assistance and Consultation in Fraudulent Schemes**: Aiming at changing the legal form or name of some contracts with the intent to deceive; or at using false or forged invoices for **tax** evasion purposes.

7. Why Combat Money Laundering?

Criminals accumulate significant sums of money by committing crimes such as drug trafficking, human trafficking, theft, investment fraud, extortion, corruption, embezzlement and tax fraud. Money laundering is a serious threat to the legal economy and affects the integrity of financial institutions. It also changes the economic power in certain sectors. If left unchecked, it will corrupt society as a whole. International laws on combating money laundering clearly and explicitly criminalize ML. This is why countries should combat money laundering. Fighting money laundering serves several purposes:

a. The Social Importance

Crime causes tangible and intangible damage to third parties, individuals and society as a whole. Money laundering can result in reducing the public's confidence in certain professions such as lawyers, accountants and notaries and economic sectors such as real estate, hospitality and banks, and other financial institutions. Investing the proceeds of crime may also distort competition between businesses and entrepreneurs. Money laundering allows the criminal to start, continue and expand activities in legitimate sectors of the economy. It may create a perception that crime pays and may also have a stimulating effect on our youth starting a criminal career.

b. To Identify Tax Crimes

Unusual transactions can be an indication of tax crimes in the past and can lead to the identification of those involved.

c. To Identify Other Crimes and Criminals

Taxing the income of criminals according to tax rules alone will not lead to the identification of potential money laundering. It will not stop crime from happening or from being profitable. The detection of unusual transactions may assist in identifying criminals and their illegal activities. Sharing information with law enforcement authorities can lead to the start of a criminal investigation.

d. To Locate and Confiscate Criminal Assets

Identifying unusual transactions can provide insight into the flow of money and the destination of laundered criminal proceeds into assets such as real estate, vehicles, yachts, and bank accounts. This will assist law enforcement authorities in seizing those assets during a criminal investigation.

8. Terrorism Financing

Terrorism financing involves the solicitation, collection, or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. More precisely, according to the International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism "if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offence within the scope of the Convention.

The primary goal of individuals or entities involved in the financing of terrorism is therefore not necessarily to conceal the sources of the money but to conceal both the financing and the nature of the financed activity.

9. Differences between ML and TF

- For ML to occur, the funds involved must be the proceeds of criminal conduct, and the mental element is normally for profit.
- For TF to occur, the source of funds is irrelevant, i.e. the funds can be from a legitimate or illegitimate source, and the mental element is normally ideology or cause-driven.
- TF occurs before the physical act of terrorism, while ML occurs after the predicate offence physical act has been completed.

10. International Code of Ethics for Professional Accountants (ICoEfPA)

The principle of professional behaviour requires professional accountants to comply with relevant laws and regulations. The Non-Compliance with Laws and

Regulations (NOCLAR) provision in the International Ethics Standards Board for Accountants (IESBA) Code creates an ethical obligation for professional accountants to speak out if they become aware of or suspect non-compliance with law and regulations, including in relation to money laundering. In January 2002, the International Federation of Accountants (IFAC) published its first paper on anti-money laundering aimed at promoting awareness of important money laundering issues and of the related professional obligations imposed on accountants. The second edition of IFAC's Paper on anti-money laundering, published in March 2004, discusses legislative and other measures taken to fight money laundering and the increased expectations that the profession monitor and detect money laundering, as well as establish and strengthen controls and safeguards against money laundering.

For more information, see the IESBA NOCLAR Factsheet, as well as installments 8 and 9 of Exploring the Code, an IFAC and IESBA series to promote understanding and awareness.

11. The National AML/CFT Laws Applicable to Professional Accountants

As a result of the growing number of highly publicized money laundering scandals, the events of September 11, 2001, and the many subsequent acts of terrorism around the world, many governments and other legal authorities in various jurisdictions have accelerated their issuance of new legislation, regulations, programs and cooperative actions, pronouncements, and enforcement steps focused on combating money laundering, terrorism financing and related financial crime. As mentioned above, the Arab States have included accountants in the AML/CFT system in response to recommendations made by the FATF.

For example, Article (14 /2-Third), of Jordan's AML and CTF Law No. 20 of 2021, stipulates that: a) The following entities shall comply with the procedures set out in this Law, regulation, instruments, and decisions issued by virtue thereof: Lawyers, other independent legal professionals and accountants when they carry out any of the following activities when they prepare or carry out financial transactions on behalf of their clients:-

- Buying and selling of real estate, or commercial stores;
- Managing of client money, securities, or other assets;
- Management of bank accounts, postal savings, investments, or securities accounts in local and international financial markets;
- Organization of contributions to the creation, operation, or management of companies;
- Creation, operation, or management of legal persons or arrangements, and buying and selling of business entities.

12. FATF Recommendations Applicable to Accountants

The basic intent behind the FATF Recommendations as it relates to accounting professionals is consistent with their ethical obligations as professionals, namely to avoid assisting criminals or facilitating criminal activity. The requirements of R. 22 regarding customer due diligence, record-keeping, PEPs, new technologies, and reliance on third parties set out in R. 10, 11, 12, 15 and 17 apply to accountants in certain circumstances. Specifically, the requirements of R. 22 apply to accountants when they prepare for or carry out transactions for their clients concerning the following activities:-

- Buying and selling of real estate, or commercial stores;
- Managing of client money, securities, or other assets;
- Management of bank accounts, postal savings, investments, or securities accounts in local and international financial markets;
- Organization of contributions to the creation, operation, or management of companies;
- Creation, operation, or management of legal persons or arrangements, and buying and selling of business entities.

R. 23 requires that R. 18, 19, 20 and 21 provisions regarding internal AML/CFT controls, measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations, reporting of suspicious activity and associated prohibitions on tipping-off and confidentiality apply to accountants when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in R. 22 above. Section III provides further guidance on the application of R. 22 and R. 23 obligations to accountants.

Countries should establish the most appropriate regime, tailored to address relevant ML/TF risks, which takes into consideration the activities and applicable code of conduct for accountants.

SECTION (III)

AML/CFT LEGAL OBLIGATIONS FOR ACCOUNTANTS:

(THE RISK BASED APPROACH)

In 2017, the Financial Action Task Force (FATF) first introduced a guidance document titled "Risk Based Approach to Combating Money Laundering and Terrorism Financing," outlining the importance of implementing the risk-based approach as part of the Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) program in international banking and other sectors. This document was revised in 2019. The FATF Recommendations 10, 11, 12, 15, 17, 18 to 23 apply to all Designated Non-Financial Businesses and Professions (DNFBPs) including accountants. In the case of accountants, these Recommendations apply in the following situations:-

- Buying and selling of real estate;
- Managing of client money, securities, or other assets;
- Management of bank, savings, or securities accounts;
- Organization of contributions to the creation, operation, or management of companies; and
- Creation, operation, or management of legal persons or arrangements and buying and selling of business entities.

The objectives of the FATF Recommendations, as they relate to Accounting Professionals, are consistent with their ethical obligation as professionals to avoid assisting criminals or facilitating criminal activity.

1. Accountants Should Know their ML /TF Risks

The Arab region is at risk of being targeted by international criminal networks to inject the proceeds of crime into the international financial system. Money laundering and financing of terrorism are not solely international crimes. Domestic criminals use a variety of methods to conceal the proceeds of their criminal activities from authorities in the Arab countries.

Undetected financial crime reduces the integrity of national and international financial systems, distorts the economy and diminishes opportunities for legitimate economic activities. The Governments loses tax revenue, while people are rewarded for criminal behaviour.

Using accounting professionals is attractive to some criminals because these professionals are required for the completion of certain kinds of transactions and because their specialist skills can be misused to assist in the laundering of criminal proceeds or funding terrorism. Accountants can add respectability and a veneer of legitimacy to transactions.

Therefore, accountants and other professionals are encouraged to develop an understanding of the ML/TF risks in the wider sectors and industries that they have business dealings with as well. Given these risks and the FATF

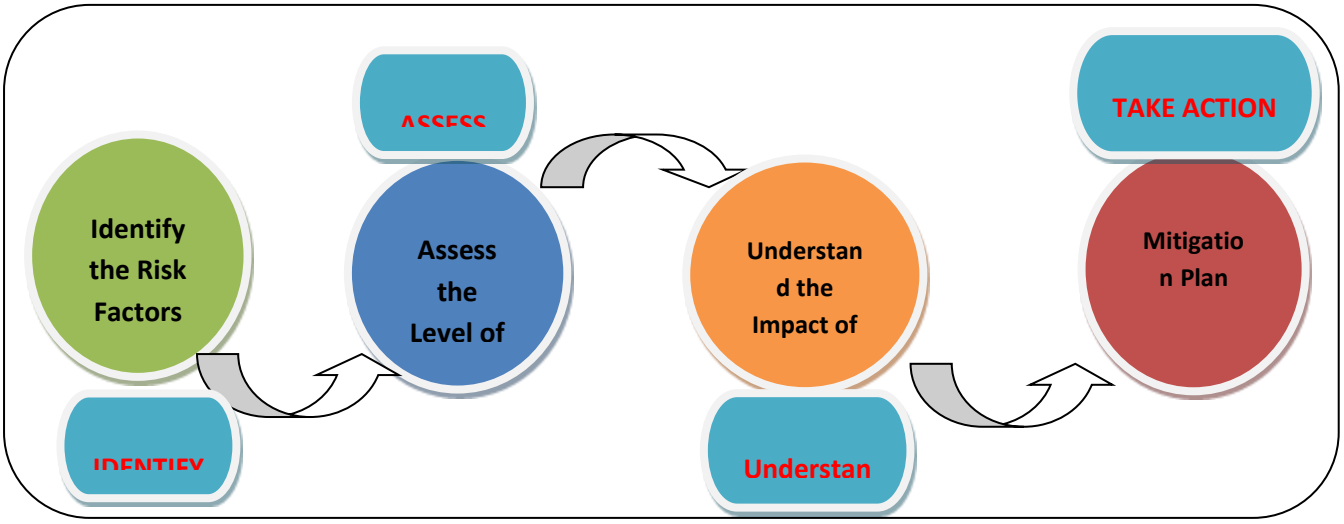
recommendations, gatekeeper professions are chosen to be engaged in the collective efforts to deter and detect these crimes. The more eyes and ears attuned to the indicators (or red flags) of these crime types, the more likely people will struggle to benefit financially from criminal activities. By expanding the AML/CFT system to include the gatekeeper professions, the IASCA intends that gatekeepers will be better able to protect themselves from customers who launder money and finance terrorism.

2. Risk-based Approach Should be Adopted

The Risk-Based Approach (RBA) to Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) is fundamental to the effective implementation of the FATF Recommendations. It requires countries, competent authorities, and DNFBPs, including accountants, to implement a RBA to:-

1. Identify the existence of risk(s) the profession is exposed to;
2. Undertake an assessment of the risk(s);
3. Understand the impact of the risk, and
4. Develop strategies to manage and mitigate the identified risk(s).

Figure 4: Risk-based Approach Implementation Groundwork



For accountants, identifying and maintaining an understanding of the ML/TF risk faced by the sector as well as specific to their services, client base, the jurisdictions in which they operate, and the effectiveness of actual and potential risk controls that are or can be put in place, will require the investment of resources and training.

The RBA is not a "zero failure" approach; there may be occasions where an accountancy practice has taken reasonable and proportionate AML/CFT measures to identify and mitigate risks, but is still used for ML or TF purposes in

isolated instances. Although there are limits to any RBA, ML/TF is a real and serious problem that accountants must address so that they do not, unwittingly or otherwise, encourage or facilitate it.

3. The Rationale for the Risk-based Approach

The RBA allows countries, within the framework of the FATF requirements, to adopt a more tailored set of measures in order to target their resources more effectively and efficiently and apply preventive measures that are commensurate with the nature of risks.

In 2012, the FATF updated its Recommendations to keep pace with evolving risks and strengthen global safeguards. Its purposes remain to protect the integrity of the financial system by providing governments with updated tools needed to take action against financial crime.

There was an increased emphasis on the RBA to AML/CFT, especially in preventive measures and supervision. Though the 2003 Recommendations provided for the application of a RBA in some areas, the 2012 Recommendations considered the RBA to be an essential foundation of a country's AML/CFT framework.

The application of a RBA is therefore essential for the effective implementation of the FATF Standards by countries and accountants.

4. Develop an AML/CFT Program

Accountants (auditors) shall develop an AML/CFT program, considering AML/CFT risks; size, complexity, and nature of the businesses. The design and implementation of such compliance program is a prerequisite to ensure compliance with the provisions of the AML/CFT Law and meeting all the obligations related to the verification of the customers' identity, record-keeping, and reporting.

The program shall include internal policies, procedures, systems, and controls aiming at preventing ML and TF, such as the following:-

- Appropriate compliance management arrangements, including the appointment of a compliance officer at the office level.
- Adequate screening procedures to ensure high standards of efficiency and integrity when appointing or employing officers and employees.
- Appropriate ongoing training program for officers and employees.
- Independent audit and review function to test compliance with AML/CFT policies, procedures, systems, and controls.
- Appropriate and ongoing review and assessment of policies.

In practice, the accountant shall develop guidance on procedures, systems, and internal controls, aiming at combating money laundering and terrorism financing, provided that it should be disseminated to the relevant employees in order to understand and apply the related requirements.

(A) **Appointing a Compliance Officer**: The compliance officer is responsible for overseeing and managing the regulated entity's compliance with the AML/CFT requirements stipulated in the AML/CFT Law, and its Implementing Regulations. The compliance officer shall particularly prepare and submit STRs to the regulator or any relevant governmental body stated in each country's law; and shall be responsible for the effective implementation of the AML/CFT Program (ensuring that appropriate policies, procedures, systems, and controls are established and developed on a regular basis, risk assessments, audit, and review is conducted to ensure the effectiveness of this Program).

If the accountant is a natural person exercising his activity in an individual establishment or office, he should personally undertake the responsibilities of the senior management and the compliance officer, within his establishment or office, and may designate one of his qualified employees as a compliance officer. If the accountant is exercising his duties under a joint liability company, branch of a company, or a non-local accounting office, the management of the company should appoint a compliance officer to manage the company's compliance with AML/CFT requirements, and submit STRs to the related regulator.

(B) **Establishment of Policies, Procedures, and Internal Controls to Ensure Compliance**: The accountant, as a DNFBP, shall develop and implement written policies, programs, and controls to ensure compliance with AML/CFT requirements. Such controls must be:-

- In a written form and made available to the concerned entities.
- Updated to keep pace with the latest applicable legislations and non-compliance cases reported, and outcomes of the independent review and testing.
- Approved by the senior management.

Generally, policies, procedures, and controls include all the obligations of the auditors and cases in which a particular procedure or measure is to be taken; in addition to the information that must be disclosed, documented, or taken into account; the measures taken and implemented to ensure compliance, the compliance timeframe, disclosure or reporting obligations and relevant methods.

(C) **Development of an Ongoing Training Program**: The accountant, as a DNFBP, must develop an appropriate training program for officers and employees, to be fully aware of their obligations by virtue of the AML/CFT **Law** and its Implementing Regulations, and of the **responsibilities** that may be incurred in case of involvement in ML and TF or non-compliance with such obligations, and of the threats, patterns, and trends of ML and TF, and of how to detect suspicious transactions and take relevant actions.

The training program should also ensure that the accountants, auditors, officers, and employees are well acquainted with the procedures, controls, and policies adopted by the office to manage and mitigate ML and TF, in addition to the role of the compliance officer and the importance of applying CDD measures and ongoing monitoring.

The accountant shall decide on the best training method, taking into account the size of the office. Several methods can be adopted such as face-to-face training, e-learning, self-learning, or a combination of more than one method. The auditor, however, should document the training program, for example by keeping record of the training attendance. It would be advisable if the training programs are supported by a test (simplified test) to ensure staff is understanding of the relevant content. Moreover, the program shall take into account the different needs of officers and employees, their expertise, qualifications, capacities, tasks, the level of supervision they are subject to (the extent of their independence while performing their functions), and the size of business and the ML/TF risks. The accountant, as a DNFBP, shall update the training program to ensure its compliance with the amended applicable legislations and relevant implementing regulations, as well as the applicable international standards and the emerging typologies of ML.

(D) **Adequate Screening Procedures to Ensure High Standards of Integrity when Appointing Employees**: The accountant, as a DNFBP, shall develop adequate screening procedures to ensure high standards of efficiency and integrity when appointing or employing officers and employees, as stipulated in the AML/CFT Rules. Enhanced screening procedures must be adopted in particular for individuals entrusted with a prominent role or position at the office of the auditor. In order to comply with this requirement, the auditor should, before appointing officers or employees, obtain information and references about the individual, his employment background, and qualifications, and confirm whether any criminal convictions or disciplinary sanctions are taken against such individual.

(E) **Independent Audit and Review Function to Test AML/CFT Program:** The accountant, as a DNFBP, should carry out periodic assessment to ensure the effectiveness of the components of the AML/CFT program: policies and procedures, ongoing training program, and risk assessment. This review aims at evaluating and documenting deficiencies and shortcomings of the AML/CFT program for future remedial actions. The review can be conducted by an independent and competent internal or external auditor, qualified to conduct the assessment. If the auditor is internal, he shall be sufficiently independent from the sections in charge of the office's operations, and not directly involved in the implementation of the activities related to the compliance program, and have a direct line of communication to the auditor (the natural person), the Board or the Chief Executive.

The methods carried out to test the effectiveness of the AML/CFT program vary depending on the scale of activity of the auditor's office or company, complexity of operations conducted, and the nature of customers. The review must be conducted regularly at least once every two (2) years.

5. Develop Checklists to Help Accountants Evaluate their Risks

Countries should develop their own checklists to help accountants evaluate the risks related to their sectors, clients, and jurisdictions in which they operate.

6. Guidance for Supervisors

This short section explains the regulatory approach you can expect from your AML/ CFT supervisors. This is to ensure that the AML/CFT system operates in a robust manner and that criminals seeking to launder money and finance terrorism are detected and deterred. More details can be found in the FATF Guidance for a Risk-Based Approach for the Accounting Profession issued in June 2019.

FATF Recommendation 28 (R.28) requires that accountants are subject to adequate AML/CFT regulation and supervision. Supervisors and SRBs (Self-Regulatory Bodies) must ensure that accountants are implementing their obligations under R.1.

A risk-based approach to AML/CFT means that measures taken to reduce ML/TF are proportionate to the risks. Supervisors and SRBs should supervise more effectively by allocating resources to areas of higher ML/TF risk.

R.28 requires that accountants are subject to adequate AML/CFT regulation and supervision, while it is each country's responsibility to ensure there is an adequate national framework in place in relation to the regulation and supervision of accountants, any relevant supervisors, and SRBs should have a clear understanding of the ML/TF risks present in the relevant jurisdiction.

According to R. 28, countries can designate a competent authority or SRB to ensure that accountants are subject to effective oversight, provided that such an SRB can ensure that its members comply with their obligations to combat ML/TF.

A SRB is a body representing a profession (e.g. accountants, legal professionals, notaries, other independent legal professionals, or TCSPs) made up of member professionals, which has a role (either exclusive or in conjunction with other entities) in regulating the persons that are qualified to enter and who practice in the profession. A SRB also performs supervisory or monitoring functions (e.g. enforcing rules to ensure that high ethical and moral standards are maintained by those practicing the profession).

Supervisors and SRBs should have appropriate powers to perform their supervisory functions (including powers to monitor and impose effective, proportionate, and dissuasive sanctions), and adequate financial, human, and technical resources.

Supervisors and SRBs should determine the frequency and intensity of their supervisory or monitoring actions on accountants on the basis of their understanding of the ML/TF risks, and taking into consideration the characteristics of the accountants, in particular their diversity and number.

Countries should ensure that supervisors and SRBs are as equipped as competent authorities in identifying and sanctioning non-compliance by its members.

Countries should also ensure that SRBs are well-informed about the importance of AML/CFT supervision, including enforcement actions as needed.

Countries should also address the risk that AML/CFT supervision by SRBs could be hampered by conflicting objectives pertaining to the SRB's role in representing their members, while also being obligated to supervise them. If a SRB contains members of the supervised population or represents those people, the relevant persons should not continue to take part in the monitoring/ supervision of their practice/firm to avoid conflicts of interest.

Supervisors and SRBs should clearly allocate responsibility for managing AML/CFT related activity, where they are also responsible for other regulatory areas understanding ML/TF risk.

SECTION (IV)

AML/CFT LEGAL OBLIGATIONS FOR ACCOUNTANTS:

CUSTOMER DUE DILIGENCE (CDD)

Customer Due Diligence (CDD) is an important measure available to accountants to prevent money laundering and avoid their practices being used by criminals to launder the proceeds of crime. In order to understand the money laundering risks that they face, accountants must verify the identities of their customers, and the nature of the business in which they are involved. The process of establishing customer identities is known as Customer Due Diligence (CDD).

1. Customer Due Diligence (CDD)

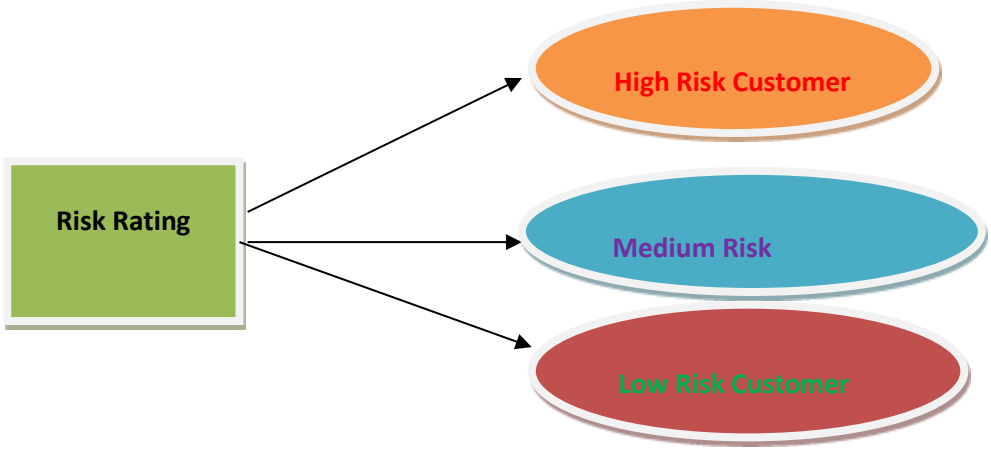
Customer Due Diligence (CDD) refers to the act of collecting identifying information in order to verify a customer's identity and more accurately assess the level of criminal risk they present. At a basic level, CDD requires firms to collect a customer's name and address, information about the business in which they are involved, and how they will use their account. In order to ensure that customers are being honest, information should then be verified with reference to official documents such as driving licenses, passports, utility bills, and incorporation documents.

CDD is a foundation of the Know Your Customer (KYC) process, which requires accountants to understand who their customers are, their financial behaviour, and what kind of money laundering or terrorism financing risk they present. CDD is a KYC process of doing background checks/investigations on a customer to assess the risk he/she poses, before engaging in a business relationship. CDD should be implemented as part of the domestic AML/CFT legislation as set out in R. 10 of the FATF's 40 Recommendations.

Criminals often seek to mask their true identity by using complex and non-transparent ownership structures. The purpose of the CDD is to know and understand a client's true identity and business activities so that ML/TF risks can be properly identified and managed. Essentially CDD is, therefore, a vital part of AML/CFT defences.

Customers can be classified as high, medium, or low risk customers.

Figure (5) Risk Rating



Accounting Professionals should apply simplified CDD measures for Low Risk Customers/Countries/Services/Industries. Normal/ Standard CDD should be applied for Medium Risk Customers/Countries/Services/Industries. Enhanced Due Diligence (EDD) should be applied for High Risk Customers/Countries/Services/Industries.

Enhanced Due Diligence (EDD) is a KYC process that provides a greater level of scrutiny of potential business partnerships and highlights risks that cannot be detected by normal/simplified CDD. EDD is therefore applicable for clients who are classified as high risk.

The FATF regards Politically Exposed Persons (PEPs), their immediate family members, and close associates as high risk clients because their positions and affiliations are susceptible to potential abuse for ML/TF and are therefore subjected to the EDD process.

In view of the change in the job description of people, the accounting professional must update his information about his clients. The following events should prompt the accounting professional to update CDD information: -

- A change in the client's identity;
- A change in beneficial ownership of the client;
- A change in the service(s) provided to the client;
- A change in the geographic location or physical address;
- A change in the client's source of wealth;
- Information that is inconsistent with the business of the client;
- A significant change in the client's business activity (includes new operations in a new country);
- Client appears on watch/sanctions list(s); and
- Suspicion or cause for concern (where doubt arises with the veracity of information provided, etc.).

The list above is not exclusive.

Customer Due Diligence involves the following basic regulatory obligations:

Customer Identification: Companies must identify their customers by obtaining personal information and data, including name, photographic ID, address, and birth certification, from a reliable and independent source.

Beneficial Ownership: When a company or third party is acting on behalf of someone else, companies should seek to establish Ultimate Beneficial

Ownership (UBO). This refers to the individual(s) who benefit from the activities of a person or group of persons.

Business Relationship: In addition to personal and beneficial ownership identification, companies must also establish the nature and purpose of the business relationship into which they are entering with the customer.

2. When is CDD Required?

Accountants should implement CDD measures under the following circumstances:

- **New Business Relationships**: Accountants must perform due diligence prior to establishing a new business relationship. The information they gather will inform any subsequent AML/CFT risk assessment and ensure that the customer is not using a fake identity to access their services.
- **Occasional Transactions**: Certain occasional transactions warrant CDD measures. These might involve amounts of money that exceed regulatory thresholds or transactions that involve entities in high-risk foreign countries.
- **Money Laundering Suspicion**: If a customer is suspected of money laundering or terrorism financing, accountants should implement additional CDD checks.
- **Unreliable Documentation**: When customers provide unreliable or inadequate identification documents, accountants should apply further CDD scrutiny to resolve discrepancies.
- **Ongoing Monitoring**: CDD is not a one-off obligation. Accountants should perform CDD periodically throughout a business relationship in order to ensure that customers' transactions are consistent with their established risk profiles.

3. Record Keeping for CDD

CDD regulations typically include a requirement for accountants to maintain records of the information they collect for at least five years. This includes copies of all identification documents (driving licenses, passports, birth certificates, etc.) and business documentation. Accountants should be able to comply quickly and efficiently with requests for records from competent authorities and enable those authorities to reconstruct individual transactions, including details of the amounts of money and types of currency involved.

4. Third-Party CDD

FATF standards permit the engagement of third parties to carry out CDD processes on behalf of accountants, including the verification of customer identities, beneficial ownerships, and the nature of business relationships. Third parties may also provide CDD record-keeping facilities.

It is important to remember that regulatory responsibility for CDD remains with the company rather than the third party. Accordingly, accountants should ensure that their CDD service provider fulfills certain compliance criteria, and is able to:

- Meet the compliance standards set out in FATF Recommendation 10
- Make copies of CDD data available upon request
- Meet FATF record-keeping requirements
- Meet location-based regulatory compliance standards

5. How to Perform Customer Due Diligence?

Following FATF guidance, accountants should implement risk-based CDD measures that reflect the specific level of risk that individual customers present. Risk-based due diligence is a way for accountants to balance their compliance obligations with their budget and resource requirements and preserve customer experiences. Under a risk-based approach, accountancy firms may deploy faster and more efficient CDD for low risk customers, and slower, more intensive, enhanced due diligence for high-risk customers – which may entail negative effects on customer experiences.

With that in mind, an effective CDD process should involve the following steps:

- Prior to beginning a business relationship, accountants should establish the identity and business activities of their new potential customer, with the goal of identifying bad actors as early as possible.
- Once a customer has been identified to a sufficient degree of confidence, accountants should categorize their risk level. This information should be stored in a digitally secure location where it can be easily accessed for future regulatory checks.
- After establishing a customer's risk category, accountants should determine whether more intensive enhanced due diligence measures are needed.

6. Enhanced Due Diligence (EDD)

Where the ML/TF risks are higher, the accountant shall perform enhanced due diligence measures commensurate with the risks identified and shall increase the intensity of monitoring the business relationship to identify unusual or suspicious activities or transactions.

6.1 When is Enhanced CDD Required?

(A) For business relationships and transactions with customers from certain countries:

- Countries identified by the National Anti-Money Laundering and Terrorism Financing Committee (NAMLC) as high-risk countries; and

circulars about the vulnerabilities of their AML/CFT regimes are issued and published on NAMLC's website.

- Countries subject to a FATF enhanced due diligence requirement. Information about these countries will be published on NAMLC's website

(B) When ML/TF risks are high, especially in the following cases:

- Complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.
- Purchase and sale transactions or transactions involving the power of attorney through non-resident customers in the State.

For other cases that are identified as high ML/TF risks for auditors.

6.2 Enhanced CDD to be Conducted by Accountants

The goal of Enhanced CDD is to learn more about the customer or transaction in order to minimize the chance that the customer or transaction is involved in ML/TF. Therefore, EDD should be tailored to fit the risk of the specific customer or transaction. Auditors should generally carry out the following enhanced measures, but may add others as appropriate:

- Increase the frequency and intensity of the business relationship monitoring;
- Obtain additional information about the customer including profession, volume of assets and information available through public databases and open sources;
- Update on an ongoing basis the identification data of the customer and the beneficial owner by undertaking reviews of existing records, particularly for high-risk categories of customers;
- Obtain additional information on the purpose and intended nature of the business relationship;
- Obtain additional information on the customer's source of wealth and funds;
- Obtain information on the purpose of the intended transactions or the conducted transactions;
- Obtain senior management approval before establishing or continuing a business relationship;
- Take enhanced measures to monitor the business relationship by furthering the intensity and degree of supervision, and identifying patterns of transactions that require additional scrutiny and review;
- Make the first payment through an account in the customer's name in a bank that is subject to similar CDD measures.

7. Simplified CDD

The accountant may conduct reduced or simplified CDD measures for customers who pose a lower level of risk.

(A) When Can Auditors Conduct Simplified CDD?

Auditors may conduct simplified CDD when all the following conditions are met:

- If the risk factors of the customer or transaction identified in the National Risk Assessment are low;
- If the risk factors of the customer or transaction identified in the self-assessment are low.
- There is no suspicion of ML/TF.
- There are no higher-risk factors, such as a link to a higher-risk jurisdiction, present.

Accountants (auditors) may also conduct simplified CDD if the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements, which ensure adequate transparency of beneficial ownership, or is a majority-owned subsidiary of such a company.

(B) What are the Simplified CDD Measures that Auditors can Conduct?

Simplified CDD can consist of taking one or all of the following actions:

- Verifying the identity of the customer and beneficial owner after the establishment of the business relationship.
- Reducing the frequency of the customer's identification updates.
- Reducing the intensity of ongoing monitoring and scrutiny of transactions based on a reasonable threshold.
- Limiting the collection of information or the conduct of specific measures, to determine the purpose and intended nature of the business relationship, and inferring instead the purpose and nature from the type of transactions carried out or from the business relationship established.

In any case, where an auditor carries out simplified CDD, he must document the risk assessment and be prepared to demonstrate to the AML/CFT section at the related department that the risk was appropriate and justified in this context.

8. Develop Checklists to Help Accountants Apply CDD

Countries should develop their own checklists to help accountants comply with both local and international AML/CFT rules and regulations, and more specifically help them apply CDD properly.

9. Ongoing Monitoring

The accountant shall conduct ongoing monitoring for each customer; and shall pay special attention to all complex, unusual, large transactions, or unusual patterns of transactions that have no apparent economic or clear legal purpose, like transactions exceeding the designated threshold or transactions not in line with the customer's type of business or occupation. The accountants shall also examine, to the extent possible, the background and purpose of the mentioned transactions, and make a record of his findings. The ongoing monitoring requires taking the following types of measures:

- Monitor the transactions conducted under the business relationship between the auditor and the customer to ensure that the transactions are consistent with his knowledge of the customer, his business and risk profile, and, where necessary, the source of his wealth and income.
- Review the records held by the auditor to ensure that the documents, data, and information collected using CDD and ongoing monitoring for the customer are kept up-to-date and relevant.

  Ongoing monitoring refers to the continuous scrutiny of business relationships. This process matters because, while occasional transactions may not initially present as suspicious, they may reveal a pattern of behaviour over an extended period of time, which necessitates a change to a customer's risk profile. Ongoing monitoring involves:

- Monitoring transactions throughout the course of a business relationship to ensure a client's risk profile matches their behaviour.
- Maintaining responsiveness to any changes in risk profile, or any factors, which might raise suspicion.
- Keeping relevant records, documents, data, and information that may be needed for CDD purposes.
- Ongoing monitoring should apply to all business relationships but, like other CDD measures, may be scaled to reflect the customer's risk profile.

Ongoing monitoring procedures involve regular review and analysis of client activities (including inquiries into the source of funds, if necessary) to make sure they are consistent with the client's operations and initial risk rating.

Ongoing monitoring of an existing business relationship should be carried out on a risk-related basis, to ensure that the accountants are aware of any changes in the client's identity and risk profile established at the on boarding stage/client acceptance.

This ongoing monitoring process ensures that documentation and information collected are kept up-to-date and relevant by undergoing reviews of existing records.

Where CDD measures create suspicion or reasonable grounds to suggest that a customer is involved in criminal activity, companies must report that information in a timely manner to their jurisdiction's Financial Intelligence Unit (FIU), via a Suspicious Activity Report (SAR). Suspicious activity reporting is the concern of the next section.

SECTION (V)

AML/CFT LEGAL OBLIGATIONS FOR ACCOUNTANTS:

SUSPICIOUS ACTIVITY REPORTING (SAR)

This section provides important information for accountants about the reporting regime that should be available in a country, what must be reported, what the reporting procedures are, and what happens after reporting.

FATF Recommendation 20 stipulates that "If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorism financing, it should be required, by law, to report promptly its suspicions to the Financial Intelligence Unit (FIU)."

FATF Recommendation 23 requires accountants to report suspicious transactions set out in R.20. R23 stipulates that "Lawyers, notaries, other independent legal professionals, and accountants should be required to report suspicious transactions when, on behalf of or for a client, they engage in a financial transaction in relation to the activities described in paragraph (d) of Recommendation 22. Countries are strongly encouraged to extend the reporting requirement to the rest of the professional activities of accountants, including auditing."

Accountants are required to report suspicious activities, as well as specific suspicious transaction, and so may make reports on a number of scenarios including suspicious business structures or management profiles which have no legitimate economic rationale and suspicious transactions, such as the misappropriation of funds, false invoicing or company purchase of goods unrelated to the company's business. As specified under Interpretive Note to R 23 (INR.23), where accountants seek to dissuade a client from engaging in illegal activity, this does not amount to tipping-off.

However, it should be noted that a RBA is appropriate for the purpose of identifying a suspicious activity or transaction, by directing additional resources at those areas that have been identified as higher risk. The designated competent authorities or Self Regulatory Bodies (SRBs) may provide information to accountants, which can inform their approach for identifying suspicious activity or transactions, as part of a RBA. Accountants should also periodically assess the adequacy of their system for identifying and reporting suspicious activity or transactions.

Accountants should review CDD if they have a suspicion of ML/TF.

1. The Reporting Regime

Arab governments should make sure that their AML/CFT Regulations include accountants as reporting entities and as such, are expected to file external reports with the FIU. Also should make sure that an internal reporting procedure that enables employees to report their knowledge or suspicions of ML/TF is in place.

An Money Laundering Reporting Officer (MLRO) must be appointed to receive these reports (See Section III.4).

It is an offence for someone who knows or suspects that ML/TF has occurred (or has reasonable grounds to do so) not to report their concerns to their MLRO (or, in exceptional circumstances, directly to the related FIU).

The MLRO has a duty to consider all such internal STRs and, if the MLRO also suspects ML/TF, then an external report must be filed to the related FIU.

While there is no definitive guidance on what constitutes 'suspicion' with regard to ML, what one is looking for is an indication that funds or assets that are the subject of a transaction came into the customer's hands as a result of illegal activity. In the case of TF, one is looking for an indication that the transaction is connected in some way with a terrorist, a terrorist group, or an act (planned or past) of terrorism.

A suspicious transaction is one that raises questions or gives rise to discomfort, apprehension, or mistrust – even without sufficient evidence. Note that the term 'transaction' includes completed, proposed, or attempted transactions.

Suspicion is not mere idle wondering, a vague feeling of unease, or a lack of understanding whether due to insufficient knowledge, ignorance, naivety, or ineffective due diligence on the part of the employee or reporting institution.

Accountants are in a position to discover ML/TF because of their expertise and involvement in the execution and facilitation of a wide range of accountancy services.

2. What Must be Reported and When?

A reporting institution shall file suspicious transaction reports and cash transaction reports, as required, to the related FIU. Suspicious Transaction Reports (STR) apply where suspicious activity is identified whilst cash transaction reports (CTR) apply to all cash transactions that exceed USD$ 10,000, or any equivalent amount in local currencies, whether suspicious or not. All reporting institutions must also submit an Annual Compliance Report (ACR).

Suspicious Transaction Reports - STRs must be filed immediately and within seven days of the date of the transaction or occurrence of the activity that is considered suspicious. Sufficient information such as the nature of and reason for the suspicion must be disclosed. Where additional supporting documentation is available, these should be provided. The STRs shall be in the form prescribed by the related FIU and the FRC will acknowledge receipt of the report.

Cash Transaction Reports - CTRs must be filed on all cash transactions equivalent to or exceeding US$ 10,000 or its equivalent in any other currency, whether or not the transaction appears to be suspicious. CTRs must be made electronically, in the week in which the transaction occurred. The FIU will acknowledge receipt of the report.

Annual Compliance Report - The AML/CFT Acts and Regulations should require reporting institutions to submit to the FIU a report indicating the institutions' level of compliance with MLA/CFT Acts, Regulations, and the institution's internal anti-money laundering rules. The report should be submitted by January 31 of the following year unless the date is varied in writing by the FIU.

3. Internal Reporting

Accountants in employment when reporting suspicious transactions should follow procedures developed by their respective employers; and if no such procedures exist, they should advise their employers to put in place reporting procedures and appoint an MLRO for reporting suspicious transactions and any other money laundering activities.

Firms should put in place internal reporting procedures. Such internal procedures should clearly set out what is expected of individuals who discover suspicions or obtain knowledge of possible money laundering. The MLRO is responsible for making decisions on whether the information contained in the suspicious transactions needs to be relayed to the FIU.

It is recommended under this guideline that all details of internal reports of suspicious activity be held by the MLRO and excluded from client files. Exclusion of information from client files assists in avoiding inappropriate disclosure of information and protects against the risk of tipping off. Client files should retain only information relevant to and required for the professional work being undertaken.

4. When Accountants Should Do SAR/STR Directly to the Regulator?

When accountants cannot complete CDD because the client refuses to provide the information or when they discover that the customers' data is fictitious or incomplete, they:

(A) Should not establish or continue the business relationship with the customer or carry out the transaction for the customer.

(B) Should strongly consider filing an STR with the relevant FIU or AML unit in relation to the customer, especially if the customer refuses to provide information, backs out of the process halfway through, or provides fictitious information.

5. Onward Reports by the MLRO to the NCA

It is the MLRO's responsibility to decide whether the information reported internally needs to be reported to the NCA. MLROs should approach external reporting with caution. When deciding what to do they should consider the following questions:

- Do I know or suspect (or have reasonable grounds for either) that someone is engaged in MLTF?
- Do I think that someone involved in the activity or in possession of the proceeds of that activity, knew or suspected that it was criminal?
- From the contents of the internal SAR, can I identify the suspect or the whereabouts of any laundered property?
- Is an application for consent required?
- Do I believe, or is it reasonable for me to believe, that the contents of the internal SAR will, or may, help identify the suspect or the whereabouts of any laundered property?
- Can I provide the information essential to an external SAR without disclosing information acquired in privileged circumstances? The privilege reporting exemption is limited to relevant professional advisers and is available only to members of professional bodies.

Further guidance on the privilege reporting exemption should be found in each country's related legislation.

The MLRO may want to make reasonable inquiries of other relevant employees and systems within the business. These may confirm the suspicion, but they may also eliminate it, enabling the matter to be closed without the need for a SAR.

There is no prescribed format for an external SAR to the NCA. Various submission methods are available. The NCA SAR Online System is the NCA's preferred submission mechanism. It is available through the NCA website and allows businesses to make SARs in a secure online environment. The NCA accepts hard copy of SARs, but will not provide a reference number in response to these.

6. What Information Should be Included in an External SAR?

The following should be regarded as essential information: -

- Name of reporter;
- Date of report;
- The name of the suspect or information that may help identify them. This may simply be details of the victim if their identity is known. As many details as possible should be provided to assist with the identification of the suspect;
- Details of who else is involved, associated, and how;

- The facts regarding what is suspected and why. The 'why' should be explained clearly so that it can be understood without professional or specialist knowledge;
- The whereabouts of any criminal property or information that may help locate it, such as details of the victim;
- The actions that the business is taking which require consent

It is also recommended that reporters:

- do not include confidential information not required by the related laws and regulations;
- show the name of the business, individual, or MLRO submitting the report only once, in the source ID field and nowhere else;
- do not include the names of the relevant employees who made the internal SARs to the MLRO;
- include other parties as 'subjects' only when the information is necessary for an understanding of the external SAR or to meet required disclosure standards; and
- highlight clearly any particular concerns the reporter might have about safety (whether physical, reputational, or other). This information should be included in the 'reasons for suspicion/disclosure' field.

7. Confidentiality

A correctly made external SAR provides full immunity from action for any form of breach of confidentiality, whether it arises out of professional ethical requirements or a legal duty created by contract (e.g., a non-disclosure agreement).

There will be no such immunity if the external SAR is not based on knowledge or suspicion, or if it is intended to be 'defensive' i.e., for the purposes of regulatory compliance rather than because of a genuine suspicion.

8. Documenting Reporting Decisions

In order to control legal risks, it is important that adequate records of internal SARs are kept. This is usually done by the MLRO and would normally include details of: -

- all internal SARs made;
- how the MLRO handled matters, including any requests for further information;
- assessments of the information provided, along with any subsequent decisions about whether or not to await developments or seek extra information;
- the rationale for deciding whether or not to make an external SAR;

- any advice given to engagement teams about continued working and any consent requests made. These records can be simple or sophisticated, depending on the size of the business and the volume of reporting, but they always need to contain broadly the same information and be supported by the relevant working papers. They are important because they may be needed later if the MLRO or some other person is required to justify and defend their actions.

For the MLRO's efficiency and ease of reference, a reporting index may be kept and each internal SAR given a unique reference number.

Reporting and the Privileged Circumstances Exemption

AML/CFT should also contain a privileged circumstances reporting exemption. Members of relevant professional bodies (which are referred to as 'relevant professional advisers') who know about or suspect MLTF (or have reasonable grounds for either) are not required to submit a SAR if the information came to them in privileged circumstances (i.e. during the provision of legal advice and acting in respect of litigation). In these circumstances, and as long as the information was not provided with the intention of advancing a crime, then the information must not be reported. The privileged reporting exemption only covers SARs and should not be confused with legal professional privilege, which also extends to other documentation and advice.

SECTION (VI)

AML/CFT LEGAL OBLIGATIONS FOR ACCOUNTANTS:

RECORD KEEPING

This section describes the reporting accountant's responsibility for the AML/CFT related record maintenance and retention. It is recognized that a "one-size-fits-all approach" does not work well for all reporting entities. However, consistent with his respective obligations, pursuant to the AML/CFT Law, the accountant shall keep records, documents, and evidence supporting his compliance with such obligations. In practice, the accountant (auditor) shall keep records as evidence of his compliance with the AML/CFT Law and its Implementing Regulations, specifically adopting and implementing the risk-based approach to mitigate risks, conduct CDD measures, and ongoing monitoring. Such records include but not limited to:

- Documents and data obtained through CDD measures.
- Account files.
- Business correspondence with the customer.
- Results of the STRs analysis undertaken.

Transaction records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. As such, record-keeping enables detecting money launderers and terrorism financiers and provides material evidence that can be traced by competent authorities in order to prosecute and track illicit actors.

1. How Long Reports Should be Kept for?

The accountant/auditor should be required to maintain all necessary records on transactions, both domestic and international, for at least (10) ten years following the completion of the transaction. The auditor should be required to keep all records obtained through CDD measures, account files and business correspondence, and results of any analysis undertaken, for at least (10) ten years following the termination of the business relationship or after the date of the occasional transaction.

Auditors must retain records beyond the end of the ten-year period mentioned above:-

(A) If they have filed with the FIU a suspicious transaction report relating to the applicant for business or customer.

(B) If they know that the applicant for business or customer is under investigation by law enforcement or judicial authorities for issues related to money laundering or terrorism financing.

Auditors should ensure that all CDD records, data, and documents on transactions and operations are available without delay to the competent authorities upon request. Auditors should also establish proper systems to ensure prompt response to the requests of the competent authorities.

2. Where Should Reporting Records be Located?

Records related to internal and external SARs 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.

3. What Do Businesses Need to Do Regarding Third-party Arrangements?

A business may arrange for another organization to perform some of its AML-related activities – CDD or training, for example. In this case, it must also ensure that the other party's record-keeping procedures are good enough to demonstrate compliance with the MLTF obligations, or else, it must obtain and store copies of the records for itself. It must also consider how it would obtain its records from the other party should they be needed, as well as what would happen to them if the other party ceased trading.

4. What are the Requirements Regarding the Deletion of Personal Data?

Regulations may require that once the periods specified in the point 1 of this guidance have expired, the business deletes any personal data unless:

- The business is required to retain it under statutory obligation, or
- The business is required to retain it for legal proceedings, or
- The data subject has consented to the retention.

The businesses are not required to keep any records for more than 10 years after the end of the business relationship.

SECTION (VII)

AML/CFT LEGAL OBLIGATIONS FOR ACCOUNTANTS:

TRAINING AND AWARENESS

1. Who Should be Trained and Who is Responsible for it?

The regulations require that all 'relevant employees' (including partners) are made aware of MLTF law and are trained regularly to recognize and deal with transactions that may be related to MLTF, as well as to identify and report anything that gives grounds for suspicion. Thought should also be given to who else might need AML training.

A designated person should be made responsible for the detail of AML training. This could be the MLRO or a member of senior management. There should be a mechanism to ensure that relevant employees complete their AML training promptly.

Someone accused of a failure-to-disclose offence has a defence if:

- They did not know or suspect that someone was engaged in money laundering even though they should have; but
- Their employer had failed to provide them with the appropriate training.

This defence– that the relevant employee did not receive the required AML training – is likely to put the business at risk of prosecution for a regulatory breach.

2. What Should be Included in the Training?

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 program itself should include:

- An explanation of the law within the context of the business's own commercial activities;
- So-called 'Red Flags' of which relevant employees should be aware when conducting business, which would cover all aspects of the MLTF procedures, including CDD (for example those that might prompt doubts over the veracity of evidence provided) and SARs (for example what might prompt suspicion); and
- How to deal with transactions that might be related to MLTF (including how to use internal reporting systems), the business's expectations of confidentiality, and how to avoid tipping off;
- The relevant data protection requirements

Training programs should be tailored to each business area and cover the business' procedures so that relevant employees understand the MLTF risks posed by the specific services they provide and the types of clients they deal with, and so are able to appreciate, on a case-by-case basis, the approach they should be taking. Furthermore, businesses should aim to create an AML culture in which

relevant employees are always alert to the risks of MLTF and habitually adopt a risk-based approach to CDD.

Records should be kept showing who has received training, the training received, and when training took place. These records should be used to inform when additional training is needed – e.g. when the MLTF risk of a specific business area changes, or when the role of a relevant employee changes.

A system of tests, or some other way of confirming the effectiveness of the training, should be considered.

The overall objective of the training is not for relevant employees to develop specialist knowledge of criminal law. However, they should be able to apply a level of legal and business knowledge that would reasonably be expected of someone in their role and with their experience, particularly when deciding whether to make an internal SAR to the MLRO.

3. When Should Training be Completed?

Businesses need to make sure that new relevant employees are trained promptly.

The frequency of training events can be influenced by changes in legislation, regulation, professional guidance, case law and judicial findings (both domestic and international), the business' risk profile, procedures, and service lines.

It may not be necessary to repeat a complete training program regularly, but it may be appropriate to provide relevant employees with concise updates to help refresh and expand their knowledge and to remind them how important effective anti-money laundering work is.

In addition to training, businesses are encouraged to mount periodic MLTF awareness campaigns to keep relevant employees alert to individual and firm-wide responsibilities.

Appendix 1

Abbreviations

For the purposes of this Guide, the following abbreviations will mean:-

ACR	Annual Compliance Report Act
CA	Chartered Accountant
CDD	Customer Due Diligence Center
CGA	Certified General Accountant
CMA	Certified Management Accountant
CPA	Chartered Professional Accountant
DNFBPs	Designated Non-Financial Businesses or Professions
EDD	Enhanced Due Diligence
FATF	The Financial Action Task Force
FIU	Financial Intelligence Unit
FRC	The Financial Reporting Center
FSRBs	Financial Action Task Force-Style Regional Bodies (FSRBs)
IFAC	International Federation of Accountants
IESBA	International Ethics Standards Board for Accountants
NOCLAR	The Non-Compliance with Laws and Regulations
MENAFATF	Middle East & North Africa Financial Action Task Force
ML	Money Laundering
MLRO	Money Laundering Reporting Officer
MLTF	Money Laundering and Terrorism Financing Numbered Account – Accounts where the identity of the holder is replaced with a multi-digit number known to the client and private bankers only
OFAC	The Office of Foreign Assets Control
PEP	Politically Exposed Person
PIP	Prominent Influential Person
RBA	Risk-Based Approach Regulations
SAR	Suspicious Activity Report Search warrant – A formal permission granted to law enforcement agencies by a court of law to search designated premises and or seize certain documents
SRBs	Self-Regulatory Bodies
STR	Suspicious Transaction Report
TF	Terrorism Financing

Appendix 2

Glossary

An Accountant: An "accountant" is now defined by the AML/ATF legislation as being a Chartered Accountant (CA), Certified General Accountant (CGA), a Certified Management Accountant (CMA) or, if applicable, a Chartered Professional Accountant (CPA), bookkeepers, tax agents and anyone else who is providing professional accounting services.

Accountancy Services: For the purpose of this guidance this includes any service provided under a contract for services (i.e., not under a contract of employment) which requires the recording, review, analysis, calculation, or reporting of financial information.

Anti-money Laundering Supervisory Authority/Unit: a body, identified by any AML/CFT adopted regulations in the Arab world, as being empowered to supervise the compliance of businesses with the AML/CFT Regulations. The professional bodies designated as anti-money laundering supervisory authorities are those mentioned in any AML/CFT regulation in the Arab world.

Arrangement: Any activity that facilitates money laundering, including planning and preparation.

Business / Businesses: A company, partnership, individual or other organization, which undertakes defined services. This includes accountancy practices, whether structured as partnerships, sole practitioners, or corporate. Business relationship a business, professional or commercial relationship between a relevant person and a customer, which— (a) arises out of the business of the relevant person, and (b) is expected by the relevant person, at the time when contact is established, to have an element of duration.

Client: Someone in a business relationship, or carrying out an occasional transaction, with a business. **Consent** Permission to carry out any activity, which would constitute a money laundering offence without that permission.

Criminal Property: The benefit of criminal conduct is where the alleged offender knows or suspects that the property in question represents such a benefit.

Customer Due Diligence (CDD): The process by which the identity of a client is established and verified, for both new and existing clients.

Defined Services Activities: Performed in the course of business by organizations or individuals as auditors, external accountants, insolvency practitioners, or tax advisers, or as trust and company services providers.

External Accountant: A firm or sole practitioner who by way of business provides accountancy services to other persons when providing such services. A family member of a politically exposed person includes a spouse or civil partner; children of that person and their spouses and partners; and parents of that person.

FATF: Financial Action Task Force, created by G7 nations to fight money laundering.

Guidance: Advice which is: (a) issued by a supervisory authority or any other appropriate body; (b) approved by the concerned body; and (c) published in a manner approved by the concerned body as suitable for bringing it to the attention of persons likely to be affected by it.

IFAC: The International Federation of Accountants (IFAC). The mission of IFAC is to serve the public interest, strengthen the accountancy profession worldwide and contribute to the development of strong international economies by establishing and promoting adherence to high-quality professional standards, furthering the international convergence of such standards, and speaking out on public interest issues where the profession's expertise is most relevant.

Internal Report: A report made to the MLRO of a business.

IASCA: The International Arab Society of Certified Accountants was established on January 12, 1984, as a non-profit professional accounting association in London, UK. It was formally registered in Amman, Jordan on February 24, 1994, under the name "The Arab Society of Certified Accountants".

MLTF (Money Laundering and Terrorism Financing): Defined for the purposes of this document to include those offences relating to terrorist finance which are required to be reported under the concerned legislation, as well as the money laundering offences defined by related laws and legislations.

MLRO Money Laundering Reporting Officer (MRLO): is the person who decides on AML reporting that may affect a company's relationship with its customer and exposure to criminal, legal, regulatory, and disciplinary action. He monitors every activity done within the AML framework.

Relevant Employee: An employee (including partner) whose work is relevant to compliance with the Regulations, or is otherwise capable of contributing to the identification and mitigation of the risks of money laundering and terrorist financing to which the business is subject, or to the prevention or detection of money laundering and terrorist financing in relation to the business.

Relevant Professional Adviser: An accountant, auditor, or tax adviser who is a member of a professional body that: (a) tests competence as a condition of

admission to membership; and (b) imposes and maintains professional and ethical standards for its members, with sanctions for non-compliance.

Required Disclosures: The identity of a suspect (if known); the information or other material on which the knowledge or suspicion of money laundering (or reasonable grounds for it) is based; and the whereabouts of the laundered property (if known).

STR/SAR: Suspicious Transaction Report/ Suspicious Activity Report. According to the Financial Action Task Force's (FATF) Recommendation 20, a suspicious transaction report (STR) or a suspicious activity report (SAR) is filed by a financial institution, MLRO, or, by a concerned citizen, to the local Financial Intelligence Unit if they have reasonable grounds to believe that a transaction is related to criminal activity.

Senior Management: means an officer or employee with sufficient knowledge of the firm's MLTF risk exposure, and sufficient authority to take decisions regarding its risk exposure (for example, having a role in determining whether high-risk clients are taken on).

Tax Adviser: A firm or sole practitioner who by way of business provides advice about the tax affairs of others, when providing such services.

Tax Compliance Services – e.g., assisting in the completion and submission of tax returns – is for the purpose of this document and included within the term 'advice about the tax affairs of others'.

Terrorism Financing Offences: These offences relate to:-

- Fundraising (s15 TA 2000 (inviting others to provide money or other property with the intention that it will be used for the purposes of terrorism, or with the reasonable suspicion that it will));
- Using or possessing terrorist funds (s16 TA 2000 (receiving or possessing money or other property with the intention, or the reasonable suspicion, that it will be used for the purposes of terrorism));
- Entering into funding arrangements making arrangements as a result of which money or other property is, or maybe, made available for the purposes of terrorism – this includes where there is reasonable cause for suspicion));
- Money laundering;
- Disclosing information related to the commission of an offence; and
- Failing to make a disclosure in the regulated sector.

Tipping Off: Any person who discloses to any other person, information or any other matter, which is likely to prejudice an investigation. Tipping off a money launderer can include: (1) changing the way the company handles the account;

(2) informing other people not related to the investigation of the suspicions; or (3) directly alerting them of suspicion.

Beneficial Owner: Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.

Competent Authorities: Competent authorities refer to all public authorities with designated responsibilities for combating money laundering and/or terrorist financing. In particular, this includes the FIU; the authorities that have the function of investigating and/or prosecuting money laundering, associated predicate offences, and terrorist financing, and seizing/freezing and confiscating criminal assets; authorities receiving reports on cross-border transportation of currency and bearer negotiable instruments (BNIs); and authorities that have AML/CFT supervisory or monitoring responsibilities aimed at ensuring compliance by financial institutions and DNFBPs with AML/CFT requirements.

Designated Non-Financial Businesses and Professions (DNFBPs): Designated non-financial businesses and professions means:

(A) Casinos (which also include internet and ship-based casinos).
(B) Real estate agents.
(C) Dealers in precious metals.
(D) Dealers in precious stones.
(E) Lawyers, notaries, other independent legal professionals, and accountants – this refers to sole practitioners, partners, or employed professionals within professional firms. It is not meant to refer to 'internal' professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to AML/CFT measures.
(F) Trust and Company Service Providers refers to all persons or businesses that are not covered elsewhere under the Recommendations, and which as a business, provide any of the following services to third parties:
  – Acting as a formation agent of legal persons;
  – Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons;
  – Providing a registered office; business address or accommodation, correspondence or administrative address for a company, a partnership, or any other legal person or arrangement;
  – Acting as (or arranging for another person to act as) a trustee of an express trust or performing the equivalent function for another form of legal arrangement;

– Acting as (or arranging for another person to act as) a nominee shareholder for another person.

FATF Recommendations: Refers to the FATF Forty Recommendations.

Legal Person: Legal person refers to any entities other than natural persons that can establish a permanent client relationship with an accountant or otherwise own property. This can include bodies corporate, foundations, associations, and other relevantly similar entities.

Legal Professional In this Guidance, the term "Legal Professional" refers to legal professionals, civil law notaries, common-law notaries, and other independent legal professionals.

Politically Exposed Persons (PEPs): Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, and important political party officials. A person who is or has been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors, and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle-ranking or more junior individuals in the foregoing categories.

Red Flags: Any fact or set of facts or circumstances which, when viewed on their own or in combination with other facts and circumstances, indicate a higher risk of illicit activity. A "Red Flag" may be used as a shorthand for any indicator of risk, which puts an investigating accountant on notice that further checks or other appropriate safeguarding actions will be required.

Self-regulatory Bodies (SRB): A SRB is a body that represents a profession (e.g. legal professionals, notaries, other independent legal professionals or accountants), and which is made up of members from the profession, has a role in regulating the persons that are qualified to enter and who practice in the profession, and also performs certain supervisory or monitoring type functions. Such bodies should enforce rules to ensure that high ethical and moral standards are maintained by those practicing the profession.

Supervisors: Supervisors refer to the designated competent authorities or non-public bodies with responsibilities aimed at ensuring compliance by financial

institutions ("Financial Supervisors") and/or DNFBPs with requirements to combat money laundering and terrorist financing. Non-public bodies (which could include certain types of SRBs) should have the power to supervise and sanction financial institutions or DNFBPs in relation to the AML/CFT requirements. These non-public bodies should also be empowered by law to exercise the functions they perform, and be supervised by a competent authority in relation to such functions.

References

1. Financial Action Task Force, (17 June 2008), Guidance on the Risk-Based Approach to Combatting Money Laundering and Terrorism Financing: High Level Principles and Procedures for Accountants, FATF, Paris. http://www.fatf-gafi.org/ publications/fatfrecommendations/documents/ fatfguidanceontherisk-basedapproachforaccountants. Html
2. https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm
3. https://www.dia.govt.nz/diawebsite.nsf/Files/AccountantsGuidelineFinal/$file/Accountants-Guideline.pdf
4. https://www.fmu.gov.pk/docs/AML_CFT_Guide_for_Accountants.pdf
5. https://www.moci.gov.qa/wp-content/uploads/2021/08/Guidance-for-Auditors_20201101.pdf
6. https: ://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf
7. The Financial Action Task Force https://www.fatf-gafi.org/
8. Middle East and North Africa Financial Action Task Force on Combating money laundering and financing of terrorism (MENAFATF) http://www.menafatf.org/
9. https://www.global-amlcft.eu/useful-links-aml-cft/
10. https://www.cbj.gov.jo/EchoBusV3.0/SystemAssets/4c677a06-7a87-45f2-9f9b-f6be53761dc9.pdf
11. https://www.sama.gov.sa/en-US/RulesInstructions/AML%20Rules/Money%20Laundering.pdf
12. https://www.ifc.org/wps/wcm/connect/e7e10e94-3cd8-4f4c-b6f8-1e14ea9eff80/45464_IFC_AML_Report.pdf?MOD=AJPERES&CVID=mKKNshy
13. https://www.fatf-gafi.org/media/fatf/documents/reports/AML-CFT-Judges-Prosecutors.pdf
14. https://www.amlu.gov.jo/Default/EN
15. https://finance.ec.europa.eu/financial-crime/eu-context-anti-money-laundering-and-countering-financing-terrorism_en
16. https://membercheck.com/aml-ctf-regulations-in-the-usa/
17. file:///C:/Users/Adli/Desktop/%D8%AF%D8%B1%D8%A7%D8%B3%D8%A9%20%D8%A7%D9%84%D9%85%D8%AC%D9%84%D8%B3%20%D8%A7%D9%84%D8%A7%D9%82%D8%AA%D8%B5%D8%A7%D8%AF%D9%8A%20%D9%88%D8%A7%D9%84%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%20%D8%A2%D8%A8%202022/03002-EX_AML-Guidelines-EN.pdf
18. https://amlexperts.com.au/industries/aml-for-accounting-firms/
19. https://www.fsa.go.jp/common/law/amlcft/210730_en_amlcft_guidelines.pdf
20. https://www.gov.uk/government/publications/anti-money-laundering-guidance-for-the-accountancy-sector
21. https://www.eba.europa.eu/esas-publish-aml-cft-guidelines

www.ascasociety.org