Unofficial translation
Main document issued by Centeral Bank of Iraq
Arabic Language

Anti-Money Laundering
Anti-Terrorism Financing
Proliferation
Regulations

Table of Contents

Introduction

Based on the provisions of Anti-Money Laundering and Anti-Terrorism Financing Law No. 39 of 2015 and the obligations it imposes on financial institutions operating in Iraq, and to achieve the objectives of the Central Bank of Iraq by strengthening the role of the banking system, updated anti-money laundering and anti-terrorism financing regulations were issued. This update takes into account all developments in the field of anti-money laundering and anti-terrorism financing, as well as the recent recommendations of the Financial Action Task Force (FATF), which included the crime of proliferation alongside the crimes of money laundering and terrorist financing. The circulars, regulations, and regulations issued by the Central Bank of Iraq and the Anti-Money Laundering and Anti-Terrorism Financing Office were also compiled to serve as a reference for all banking and non-banking financial institutions to combat these crimes.

These regulatory regulations were issued taking into account global developments in combating money laundering, which have been linked to combating the financing of terrorism, following the updating of the 40 Recommendations on Combating Money Laundering and the Financing of Terrorism issued by the Financial Action Task Force (FATF). These recommendations are considered international standards in combating these two phenomena, to which countries must adhere. They also took into account the direct outcomes approved by the FATF and the guidelines issued by it.

This necessitated the issuance of these regulatory regulations for banks to combat this phenomenon. These regulations took into account these developments and consolidated existing practices in the field of opening accounts, conducting banking operations, and procedures to combat this phenomenon. These efforts were also improved and activated to keep pace with global changes in this field, ensuring strict adherence to these regulations by banks and branches of foreign banks operating in Iraq.

The aforementioned regulations also apply to all branches abroad of banks operating in Iraq, taking into account that if the obligations contained in these regulations differ from those imposed in the host country, the stricter obligations shall be applied, provided that they do not conflict with the legislation or regulatory instructions applicable in the host country, taking into account informing the Central Bank of Iraq in the event of the inability to implement sound measures to combat money laundering and terrorist financing as a result of such legislation or instructions.

Section 1: The Purpose of These Regulations

1. These regulations aim to ensure banks' compliance with the provisions of Anti-Money Laundering and Terrorist Financing Law No. (39) of 2015 and all related instructions and regulations.
2. Protect the banking sector from money laundering and terrorist financing operations by ensuring that all banks comply with the laws, regulations, policies, regulations, procedures, bylaws, and principles that ensure the prevention, detection, and reporting of money laundering and terrorist financing activities in accordance with local and international standards.
3. Protect banks from illegal operations and prevent their exploitation as conduits for illegal operations and transactions that may involve money laundering, terrorist financing, or any other illegal activities.
4. Enhance the integrity of the banking sector and protect its reputation and integrity to ensure the protection of its customers.

Section 2: Scope of Application of Regulations
These regulations apply to all banks licensed by this Bank and operating in the Republic of Iraq.

Section 3: Inconsistent Instructions and Regulations
Any regulations or circulars that are inconsistent with these regulatory regulations shall be suspended from the date of their entry into force and replaced.

Section 4: Entry into Force
These regulations shall become effective from the date of their signature.

Chapter 1: Concepts, Definitions, and Phases of Money Laundering

Article 1: Definitions

Without prejudice to the definitions contained in Law No. (39) of 2015 on Combating Money Laundering and the Financing of Terrorism and the definitions contained in its Executive Regulations, and for the purposes of these regulations, the following words and phrases, wherever they appear, shall have the meanings indicated opposite each of them.

1. The Law: Law No. (39) of 2015 on Combating Money Laundering and the Financing of Terrorism.
2. The Office: The Anti-Money Laundering and Counter-Terrorism Financing Office at the Central Bank.
3. Funds: Assets of any type, whether physical, intangible, or digital, movable or immovable, currencies of all kinds, foreign or local, securities, commercial papers, instruments, and documents proving ownership of funds or any right related thereto, and other revenues or values arising from or resulting from these assets.
4. Money laundering: Any act intended to conceal or disguise the illicit source of funds or proceeds derived from a predicate crime, or to assist the perpetrator in evading punishment.
5. Terrorist financing: The act defined in Article 1 (tenth) of the law.
6. Regulatory authorities: The authorities responsible for licensing, authorizing, or supervising financial institutions and designated non-financial businesses and professions to ensure their compliance with the requirements of combating money laundering and terrorist financing, such as the Central Bank of Iraq.
7. Beneficial owner: The natural person who owns or exercises ultimate direct or indirect control over the customer or the natural person on whose behalf the transaction is conducted, as well as the person who exercises ultimate effective control over a legal person or legal arrangement.
8. High-Risk Persons:
    - Foreign politically exposed persons (PEPs) are individuals entrusted with prominent public functions in a foreign country, such as heads of state or government, high-ranking politicians, high-ranking government officials, judicial and military officials, senior executives of state-owned enterprises, and important political party officials.
    - Domestic politically exposed persons (PEPs) are individuals entrusted with prominent public functions domestically, such as heads of state or government, high-ranking politicians, high-ranking government officials, judicial and military officials, senior executives of state-owned enterprises, and important political party officials.
    - PEPs entrusted with prominent functions of an international organization are members of senior management, i.e., directors, deputy directors, board members, or equivalent positions. This definition does not apply to individuals holding middle or lower positions in the aforementioned categories.
9. Due Diligence Measures: Exerting efforts to identify and verify the identity of the customer and the beneficial owner, and continuously monitoring transactions occurring within an ongoing relationship, as well as identifying the nature and purpose of the future relationship between the financial institution, non-financial institution, or designated profession and the customer.
10. Ongoing Relationship: A financial or banking relationship between a bank and a customer that, upon its inception, is expected to extend over a period of time and include multiple transactions. A continuing relationship includes any financial or banking relationship related to one of the activities included in the definition of financial institutions and non-financial institutions and connected to the

activities and services the bank provides to its customers whenever the bank anticipates the relationship will extend over a period of time.

11. A shell bank (fake bank) is a bank that has no physical presence in the country in which it was established and licensed, and that is not affiliated with any financial services group subject to the supervision and oversight of an effective regulator.
12. Physical Presence: A bank's physical presence is ensured by:
    - A fixed business location to receive customers and conduct its business effectively, not just a local agent or low-level employees.
    - Existence of actual management
    - Maintaining transaction records
    - Subject to inspection by regulatory and supervisory authorities, whether in the country in which it was established or in the country in which it operates.
13. Correspondent Banking: The provision of banking services from one bank to another correspondent bank.
14. Non-Profit Organization: Any legal entity established in accordance with the provisions of applicable laws whose primary purpose is to provide social or voluntary services without seeking profit-making, profit-sharing, or personal gain, and which collects or disburses funds for charitable, religious, cultural, educational, or social purposes.
15. Customer: Any person who conducts or initiates any of the following activities with a financial institution or designated non-financial business or profession: arranging, opening, or executing a transaction, business relationship, or account for him; participating in signing a transaction, business relationship, or account; allocating or transferring an account, rights, or obligations under a transaction; and authorizing a transaction or controlling a business relationship or account.
16. Transient Customer: A customer who does not have a continuous relationship with the bank.
17. Non-Resident Customer: A natural or legal person who resides or is usually based outside Iraq or who has not completed one year of residence in Iraq, regardless of that person's nationality. This does not apply to individuals who have a permanent economic activity and permanent residence within the Republic of Iraq, even if they reside there intermittently.
18. Wire Transfer: Any transaction conducted on behalf of the originator of the transfer through a subject entity via digital means with the aim of making a sum of funds available to a beneficiary in a beneficiary subject entity, regardless of whether the originator and beneficiary are the same person.
19. Transfer of Funds or Value: A financial service that includes Accepting cash, checks, or other monetary instruments or reserves and paying an equivalent amount in cash or in any other form to a beneficiary by means of a call, message, transfer, or through a clearinghouse network to which the money or value transfer service belongs. Financial transactions conducted by such services may involve one or more intermediaries and a final payer to a third party. They may also include any new payment methods. These systems often have links to specific geographic areas.
20. Legal Arrangements: A relationship established by contract between two or more parties that does not result in the creation of a legal entity, such as trust funds or other similar arrangements.
21. Specified Non-Financial Businesses and Professions. These businesses and professions include lawyers, notaries, dealers in precious metals, jewelers, real estate brokers, accountants, and trust funds.
22. Digital banking services include all digital banking services such as internet banking, telephone banking, and online payment services.
23. Bank cards include all digital payment cards of various types: credit, debit, prepaid, and prepaid cards.

24. Anti-Money Laundering Systems: A set of systems that develop software solutions for receiving, processing, and analyzing customer transactions and deposits to determine the extent to which these transactions and cash deposits correspond to their cash flows and income.
25. Domestic and International Sanctions: Sanctions imposed on specific individuals or institutions, including asset freezes and embargoes to prevent funds or other assets from being made available, directly or indirectly, to sanctioned individuals, entities, groups, or organizations.
26. The Digital Anti-Money Laundering and Countering the Financing of Terrorism (GOAML) System: An integrated software solution for combating money laundering and the financing of terrorism developed by the United Nations Office on Drugs and Crime (UNODC) for use by the Office for Anti-Money Laundering and Countering the Financing of Terrorism (UNODC) for data collection, management, analysis, document management, workflow, and other statistical needs. This system receives reports in cases of suspected money laundering and terrorist financing digitally and in real time, replacing paper reports.

Article 2: Phases of Money Laundering

The money laundering process involves three main, interconnected phases, as follows:

1. Phase One: The Deposit Phase: This Phase involves depositing illicit funds, often in cash, into several bank accounts, or investing them in legitimate investment projects or purchasing stocks and real estate.

2. Phase Two: The Covering Phase: This phase involves moving illicit funds domestically or abroad, often to countries with strict banking secrecy laws. These operations are often complex, making it difficult to trace the source of the illicit funds. This is accomplished through the use of available banking operations and shell company accounts that engage in no real activity other than receiving money transfers and then re-sending them to other parties.

3. Phase Three: Integration: In this phase, illicit funds are reinjected into the local and global economy as legitimate funds through the purchase of stocks, bonds, real estate, and other assets, and the establishment of investment projects, etc. (i.e., as legitimate investments, particularly in developing countries). All evidence that could indicate the true illicit source of the funds is obliterated, making them appear as funds resulting from legitimate activities. Money launderers are then able to use and benefit from these funds.

Article 3: The Concept of Terrorist Financing

The various methods used in money laundering are essentially consistent with those used to conceal the sources and uses of terrorist financing. Funds used to support terrorism can originate from legitimate sources, criminal activities, or both. However, disguising the source of terrorist financing is crucial, regardless of whether it originates from legitimate or illicit sources.

Article 4: The Concept of Preventing Proliferation

Recent updates to the definition of money laundering and terrorist financing, as defined by the Financial Action Task Force (FATF), have included the concept of preventing proliferation. This crime is no less serious than the two previous crimes. Banks and non-bank financial institutions must exercise heightened due diligence regarding any entities and individuals suspected of dealing with high-risk entities or countries known to engage in proliferation. They must also act in accordance with United Nations

Security Council resolutions regarding countries, entities, and individuals banned from international transactions due to proven direct or indirect involvement in proliferation crimes.

Chapter 2: Basic Principles for Combating Money Laundering/Terrorist Financing

Article 1: Know Your Customer (KYC) Principle

In accordance with this principle, banks must identify all their customers in a manner commensurate with their risk levels, as follows:

1- Individuals: The bank must follow at least the following procedures to identify the customer:

a. Ensure that the customer has completed the Know Your Customer (KYC) form for opening all types of accounts, prepared by the bank.
b. The bank must obtain the following documents: (a copy of the personal identification card, passport if available (if unavailable, a pledge to provide it, and other identification documents). For non-Iraqis, a copy of the passport must be obtained, provided the customer has a valid residency permit in the Republic of Iraq.
c. Obtain the names, information, and nationalities of the persons authorized to deal with the account, and retain copies of the documents proving this.
d. Obtain detailed information about the beneficial owner in accordance with the Beneficial Ownership Guide issued by the Anti-Money Laundering and Terrorism Financing Office. This information must not be less than that of the customer opening the account.
e. Obtain the names and addresses of legal representatives of incapacitated persons and retain copies of the supporting documents or any other documents not mentioned, as the bank may deem necessary.
f. The bank must ensure that the competent employee has reviewed the original documents and signed the retained copies, indicating that they are true copies.
g. Stamp the supporting documents obtained from the customer with a special stamp bearing the phrase "These documents are used exclusively for the purpose of opening the bank account."
h. The account opening form must be signed by the (form organizer, branch liaison officer, reporting department manager or assistant at the main branch, branch manager). The form data must be updated periodically, and the Anti-Money Laundering and Terrorism Financing Office must be notified if any suspicions arise. The customer must not be notified.
i. Obtain accurate information about the person requesting the account, their activity, and profession.
j. Take all necessary measures to verify the beneficial owner of the account.
k. Taking the necessary measures included in these regulations for all high-risk individuals to ensure that the customer is a person exposed to risk by virtue of their position.
l. Obtaining a pledge from the customer to update their information immediately upon any changes or upon the bank's request, provided that the period is no less than six months.
m. The bank must verify the accuracy of the customer's information by reviewing the original documents submitted by the customer and obtaining a validation from the relevant authorities in certain cases where this is required.
n. Completing any other information not mentioned, which the bank may deem necessary.

2- Legal Person (Jurisdictional): If the client is a legal person, the information and documents proving the nature of the person, its legal entity, and the validity of the documents and papers supporting the existence of this entity, its name, domicile, financial structure, and detailed activities, as well as the information of the persons authorized to deal with the account by official authorization, as well as the names and addresses of the major shareholders, members of the Board of Directors, and the executive management, shall be completed by following at least the following procedures:

a. Ensure that the client has completed the Know Your Customer (KYC) form for requesting the opening of all types of accounts prepared by this bank. These forms must be divided between the head office and branches, and must include a minimum of the information contained in the circulars for all account opening forms, signed by the competent employee.
b. The bank must complete the following documents:
c. A true copy of the articles of association and the certificate of incorporation issued by the Companies Registration Department.
d. A true copy of the commercial register.
e. The name and address of the owner, and the names and addresses of partners or shareholders who each own more than 10% of the organization's or company's capital.
f. The names and addresses of the company's authorized signatories and executive directors.
g. Specimen signatures of persons authorized to deal with the account.
h. A written acknowledgment from the customer stating the identity of the beneficial owner of the account or the economic right holder of the intended transaction. This acknowledgment should include the customer's full name, surname, and place of residence, as well as information about his or her financial status.
i. The bank must identify the beneficial owner and take appropriate measures to verify his or her identity, such as reviewing data or information obtained from the issuing entity, to ensure that the parties are convinced that they are aware of the beneficial owner's identity. When identifying the beneficial owner of a legal entity, the following should be taken into account:
    - Natural persons who own a controlling stake in the legal entity.
    - Natural persons who control the legal entity or legal arrangement through any other means, and ensuring that the founder or any other person in the ownership and management structure is not included in the international and local ban and sanctions lists published on the official website of the Anti-Money Laundering and Terrorism Financing Office and all other relevant authorities.
    - If there is any indication of suspicion, the authenticity of the originals submitted by the legal entity shall be verified.

j. The decision of the Chairman of the Board of Directors of the company to open the account and the person(s) authorized to use the account, along with identifying them.
k. A copy of the identity card (national) or passport of the owner of the organization or company.
l. Joint shareholders or partners whose share in the company's capital is (10) or more and who are authorized to sign on behalf of the company.
m. Documents proving the organization or company's authorization for the person(s) representing it.
n. Any other documents not mentioned that the bank may deem necessary.
o. The bank must ensure that the competent employee has reviewed the original documents and signed the retained copies, indicating that they are true copies. If any indication of suspicion is found regarding the accuracy of the data, information, documents, or records provided, the bank

must take appropriate measures to verify their authenticity by all possible means, including contacting the competent issuing authorities.

p. The purpose of the account transaction and the establishment of the business relationship.
q. Joint-stock companies: In addition to fulfilling the documents and requirements mentioned above, the names and addresses of the chairman of the board of directors, the general manager, and the financial manager must be completed.
r. Take the necessary measures to verify the beneficial owner of the account.
s. Take the measures mentioned within these regulations to ensure that the customer is a person exposed to risks by virtue of his position.
t. The bank must pay special attention to legal persons and verify their actual existence by obtaining a copy of the company's latest financial report or financial statements, or by verifying through any other available sources.
u. The customer must provide a pledge to update their information immediately upon any changes or upon the bank's request, provided that the update period is no less than six months.
v. Verify the accuracy of the customer's information and review the original documents submitted by the customer.
w. Complete any other information not mentioned that the bank deems necessary.

3- Non-profit organizations: The bank must not open any accounts for non-profit organizations unless the following documents and information are provided:
   a. A letter issued by the entity regulating the work of these organizations confirming their identity and authorizing them to open bank accounts.
   b. A true copy of the articles of association.
   c. A true copy of the licensing decision.
   d. The name and legal form of the organization.
   e. The address of the headquarters and branches.
   f. The telephone number and email address, if available.
   g. The purpose of the transaction, the sources and uses of its funds, and any other information requested by the competent authorities.
   h. The names and addresses of the authorized signatories on behalf of the organization.
   i. Specimen signatures of the persons authorized to deal with the account, in addition to the necessity of identifying the authorized persons in accordance with the customer identification procedures mentioned above.
   j. Ensure that the data on the special form prepared by the bank to verify the identity of customers of non-profit organizations is completed when opening accounts of all types.
   k. The bank must exercise special care regarding non-profit organizations and associations, ensuring their actual existence and that account applicants are the true owners of the organization or association. It must also implement enhanced due diligence procedures for non-profit organizations in the following cases:
   l. Measures must be taken to determine whether there is a relationship between the organization and high-risk senior officials.
   m. Establish business policies and procedures to manage risks related to high-risk officials who have a direct or indirect relationship with non-profit organizations by incorporating this policy into the bank's anti-money laundering and counter-terrorism financing policies and procedures.
   n. Take strict and sufficient measures to verify the sources of funds of non-governmental organizations that have a business relationship with high-risk officials.

o. Activities and businesses that do not have a clear social purpose or legal basis. Strict oversight procedures must be put in place to determine the background and circumstances surrounding this activity and any deviations, and these findings must be recorded in special records.
p. Transactions carried out by individuals or non-profit organizations located in or belonging to countries that do not have systems in place to combat money laundering and terrorist financing, particularly if these countries do not implement, or insufficiently implement, the global regulations on combating money laundering and terrorist financing published on the Financial Action Task Force's website.
q. When there is any indication of suspicion regarding a non-profit organization related to a money laundering or terrorist financing operation, or a situation that raises doubts regarding the validity and accuracy of previously obtained information and data.
r. Activities and businesses carried out by the organization suspected of illegal financing, whether through physical, digital, or other means.
s. Activities and businesses financed or supported by high-risk individuals.

4- Verification of the accuracy of data: The bank must verify the accuracy of the data provided about the customer by reviewing the original documents submitted by the customer and obtaining a copy thereof. The bank must have the relevant employee sign each document after verifying it with the original, indicating that it is a true copy.

5- Dealing by Agency: In the event that a person deals with the bank on behalf of the client, whether the client is a natural person or a legal entity, the bank must ensure the existence of a legal power of attorney or legal authorization approved by the competent authorities. It is necessary to retain the power of attorney and authorization, or a true copy, and to identify and verify the identity of the agent and principal in accordance with the aforementioned customer identification procedures.

6- Correspondent Banks: Due Diligence Procedures for Correspondent Banks or Financial Institutions. When establishing a business relationship with a financial institution or correspondent bank, the bank must implement the customer due diligence procedures mentioned above for legal entities, in addition to the following:
a. Obtain the approval of the bank's senior executive management before establishing a relationship with correspondent banks.
b. Gather sufficient information about the correspondent bank, as well as its ownership and management structure, to gain a complete understanding of the nature of its business and, based on publicly available information, determine its reputation and the type of oversight it exercises. This also includes determining whether the correspondent bank, any of its board members, or controlling shareholders have been subject to investigations into money laundering or terrorist financing crimes, or to any administrative sanctions or measures.
c. Completing data that demonstrates the correspondent bank's compliance with its local legislation and regulatory regulations, the due diligence standards applied to its customers, its efforts to combat money laundering and terrorist financing, and the extent to which the correspondent bank has effective internal policies and procedures in this regard. This should be done through a questionnaire or survey. Correspondent banks or financial institutions are required to answer the questions included in the questionnaire, which clarify their compliance with their local legislation and regulatory regulations, the identity verification standards and procedures applied to their customers, their efforts to combat money laundering and terrorist financing, and the extent to which they have effective internal policies and procedures.

d. Defining in writing the responsibilities of each financial institution or correspondent bank for combating money laundering and terrorist financing.
e. Ensuring that the financial institution or correspondent bank is subject to effective regulatory oversight by the competent authorities.
f. Documenting the information, documents, and written agreements obtained from the financial institution or correspondent bank and making them available to the competent authorities when necessary.
g. The bank must ensure that financial institutions or correspondent banks that maintain correspondent payment accounts implement due diligence procedures on their customers who have access to those accounts and are able to provide documents, data, and information related to due diligence measures and ongoing monitoring upon request within an acceptable timeframe or without delay.
h. Periodically review transactions conducted on the correspondent bank's account to ensure that such transactions are consistent with the purpose for which the account was opened.
i. When conducting due diligence procedures to identify the correspondent bank, the bank must determine its risk level based on the information available to it, including the following:
    - The presence of any regulatory reservations regarding the bank's anti-money laundering and counter-terrorism financing systems or the risk management systems that may result from them.
    - Whether the correspondent bank's head office is located in a high- or low-risk country.
    - The extent to which the correspondent bank provides private banking services.
    - The extent to which high-risk individuals, by virtue of their public positions, hold accounts with the correspondent bank.
    - Not entering into correspondent relationships with fictitious banks/financial institutions, or with institutions that provide correspondent services to fictitious banks.

7- Legal Arrangement

First: Paragraph 19 of the Anti-Money Laundering and Terrorism Financing Law No. 39 of 2015 defines a legal arrangement as a legal relationship established by a contract between two or more parties that does not result in the creation of a legal entity, such as trust funds, trusts, or other similar arrangements.

Trust Funds: A legal relationship that does not create a legal entity, but rather is established by a written document whereby a person places funds under the management of a trustee for the benefit of one or more beneficiaries or for a specific purpose.

In general, the term trust refers to the legal relationship that arises between living people or upon death. A person, known as a founder or testator, places assets under the control of a trustee or guardian for the benefit of a beneficiary or for a specific purpose. It is also known as a structure whereby a person (the founder or testator) transfers assets or property to another person, whom they entrust to dispose of them according to their instructions and for the benefit of beneficiaries. These are the persons designated by the founder or testator to receive assets, gains, or income at a specific time, or they can be a specific category of unspecified persons. Trusts consist of three parties:

1. The testator, who owns the assets or funds and wishes to establish the trust fund according to its specific terms and as they see fit. They transfer the assets or property to the trustee.
2. The trustee, who is the person to whom the assets are transferred and who is appointed to manage the assets and funds according to the terms specified by the testator.
3. The beneficiary, who is the person who will benefit from the proceeds of the management of the assets and funds.

Among the structures that the Financial Action Task Force considers a form of legal arrangement are certain types of endowments. Endowments can take the following forms:

- Private (family) endowments: These are endowments intended to benefit individuals or their descendants, and may become charitable endowments upon the discontinuation of the endowed endowment.
- Charity endowments: These are endowments intended for charitable and charitable purposes, and are administered by governments (either directly or through a trustee) in accordance with the laws of the endowment offices. They represent the majority of endowments in Iraq.
- Joint endowments: These combine both family (family) and charitable endowments.

Second: The danger of legal arrangements lies in their ability to mitigate money laundering and terrorist financing. The reason behind this is the difficulty of tracking and identifying the true beneficiary behind these arrangements.

Based on the above, a legal entity or legal arrangement cannot be the beneficial owner. All banks and financial institutions dealing with legal arrangements must examine the structure of the legal entity or legal arrangement to determine its beneficial owner (a natural person). The hierarchy must be followed until a natural person is identified as the beneficiary or ultimate beneficiary of the natural person or legal arrangement. This is because any legal entity or arrangement must ultimately be subject to the control of a natural person. All banks must not open any accounts or conduct any banking relationship or transaction with legal arrangements, including endowments, unless they have obtained the following:

1. A letter from the entity responsible for the endowment confirming its identity and authorizing the entity to open bank accounts.
2. A certified copy of the endowment deed issued by the competent personal status court.
3. The name, legal form, and type of the endowment.
4. The address of the endowment and its nearest point of reference.
5. The telephone number of the person responsible for managing and supervising the endowment.
6. The purpose of the transaction, the sources and uses of its funds, and any other information requested by the competent authorities.
7. The names and addresses of those authorized to sign on behalf of the legal arrangement.
8. Specimen signatures of the persons authorized to deal with the account, in addition to the necessity of identifying the authorized persons in accordance with the customer identification procedures mentioned above.
9. Ensure that the data on the special form prepared by the bank to verify the identity of customers for non-profit organizations is completed when opening accounts of all types.
10. Evidence of the sources of the endowment assets.

11. The place of residence of the trustee of the endowment and any assets held or managed by him/her in relation to any trustees or custodians with whom he/she has a business relationship or for whose account he/she performs occasional transactions, and any other information the institution deems necessary to obtain. Banks and financial institutions must also exercise due diligence regarding legal arrangements by doing the following:

    a. Identify all parties involved in the legal arrangement, including the trustee, the testator, the beneficial owner, the agency holders, and all parties dealing directly or indirectly with the bank.
    b. Conduct a search and investigation of local and international sanctions and ban lists on all parties to the legal arrangement.
    c. Identify the sources of all legal arrangement funds and ensure that these funds are legitimate and derived from legitimate activities, and that there are no suspicions of money laundering or terrorist financing.
    d. Verify whether the beneficiaries or parties involved in the legal arrangement include persons exposed to risk by virtue of their position, by fully understanding the ownership structure of the legal arrangement.
    e. Identify the identities of the founding trustee (who owns the assets or funds), the trustee (the person to whom the assets are transferred), the beneficiary (the person who benefits from the proceeds of managing the assets or funds), the supervisor (if any), and any other natural person who exercises effective and ultimate control, directly or indirectly.
    f. The identity of any other natural person who exercises effective or actual control over the Waqf, whether through the chain of control, ownership, or through other means. The Beneficial Ownership Guide issued by the Anti-Money Laundering and Terrorist Financing Office must also be used to determine the criteria used to determine the beneficial owner of legal arrangements in all their forms.

Article 2: The Principle of the Risk-Based Approach

The risk-based approach, based on Recommendation 1 of the Financial Action Task Force (FATF) Forty Recommendations, assesses and identifies the risks facing the country in the area of combating money laundering and terrorist financing. Accordingly, financial institutions must design and implement appropriate measures to mitigate these risks, by following the following:

First: Risk Assessment

1- The bank must develop a risk-based approach to the monitoring process that is appropriate to its business, the number of customers, and the types of transactions.
2- The bank must classify its customers and products according to the degree of money laundering and terrorist financing risks.
3- The bank must exercise special care in dealing with cases that represent a high degree of risk.
4. The bank must establish the necessary procedures to address these risks in accordance with these levels.
5. The bank must classify the risk levels into high, medium, and low.

Second: Risk Identification

1. The bank must review the classification of customers according to the risk levels related to money laundering and terrorist financing at least once every two years, or if subsequent changes occur within the two years that require it.
2. Financial institutions must acquire and adopt specific systems to combat money laundering and terrorist financing (AML) to measure and identify risks related to customers, products, service delivery channels, and geographic area risks. This system must be directly linked to the comprehensive banking system (Core banking system) on the one hand, and to the Automatic Integration platform for investigating and investigating those listed on local and international sanctions and ban lists on the other hand.
3. Prepare a detailed matrix upon which the aforementioned system relies, taking into account risks related to high-risk customers, such as non-designated financial businesses and professions, persons exposed to risk by virtue of their position, charitable organizations, non-resident customers, etc.
4. Adopting the scenarios prepared by the Anti-Money Laundering and Counter-Terrorism Financing Office within the Anti-Money Laundering (AML) system and working to update this system with any scenarios issued by the office through periodic follow-up.

Third: Implementing Measures

1. When classifying risks in the business relationship between the bank and the customer, the bank must ensure that the risk management system includes policies and procedures based on identifying, assessing, controlling, and reporting risks, provided that this system covers all areas of risk.
2. When characterizing the risks in the business relationship between a bank and a customer, the bank must consider the following four risk elements at a minimum (customer risks, product risks, service channel risks, and geographic risks):

    a. Customers Risk
        - The bank must assess and document the risks of money laundering, terrorist financing, and other illicit activities posed by various customers. The intensity of due diligence and ongoing monitoring required for a specific type of customer must be proportionate to the apparent or potential degree of risk posed by the business relationship with the customer. The bank must also have policies and procedures in place to address these risks.
        - The bank must ensure that enhanced due diligence procedures and ongoing monitoring are in place if there is suspicion that a customer is an individual, charity, or non-profit organization linked to terrorist acts or terrorist financing, or a terrorist organization associated with them. The ownership structure of suspected legal entities must be understood to determine the beneficial owner behind that entity, or if the individual or entity is subject to sanctions, is on lists circulated to banks, or is exposed to risks by virtue of their position or related to issues related to combating money laundering and terrorist financing.
        - A decision to enter into a business relationship with non-profit organizations or customers requiring enhanced due diligence measures should not be made until the approval of senior executive management has been obtained after the enhanced measures have been completed. The following are some of the factors that guide the bank's identification of such risks:

i. Customer-related risks:
- Customers whose beneficial owner is difficult to identify, for example:
- Due to the complexity of their ownership structure in the case of legal entities.
- Customers whose reputation or past dealings are tainted.
- Non-resident customers. Customers who are considered high-risk individuals by virtue of their public positions or those associated with them, and foreign customers.
- Customers who are non-resident citizens of other countries.
- Customers exposed to risk by virtue of their position.
- Customers specializing in real estate trading.
- Customers specializing in precious metals trading.
- Customers involved in car trading.
- Any customer working in other unspecified financial businesses and professions.

ii. Risks related to customer transactions:
- Transactions not being proportional to the stated purpose of the transaction.
- Services requested from customers not being proportional to the nature of their business.
- Conducting complex or large transactions without a clear justification.
- Transacting with an institution located far from the customer's residence or place of work without a clear justification.
- Multiple accounts and/or business relationships with customers at the bank, or with more than one institution located in the same area, without a clear purpose.
- Dealing in large amounts of cash even though the customer's business is not a cash-intensive activity.
- Customers whose transactions with the bank undergo a significant change without clear justification, or the bank receives information about their involvement in illegal activities.
- Unjustified use of intermediaries in transactions.
- Customers requesting excessive confidentiality regarding certain transactions.
- Indirect transactions and those conducted using modern technological means.

iii. Risks related to customer activity sectors: Activities characterized by cash-intensive transactions, including activities related to the provision of financial services, such as money transfer companies, exchange companies, charities and other non-profit organizations, dealers in precious metals, gemstones, antiques, and works of art, real estate brokers, and real estate companies.

b. Product Risk
- The bank must assess and document the risks of money laundering, terrorist financing, and other illicit activities arising from the products it offers or proposes to offer to its customers. These products may include savings accounts, money transfer products, correspondent accounts, wire transfers, etc. The bank must also have a methodology for classifying its business relationships with its customers based on the different types of products it offers or proposes to offer.
- Risks related to products that could be exploited for money laundering or terrorist financing include new or innovative products or services, whether offered by the bank or to which it is a party. These include services that do not disclose a significant amount of

- information related to the identity of their users, or those of an international nature, such as online banking services, stored-value cards, and international digital transfers.
- All operations and transactions conducted by the bank must be monitored. Monitoring must include the number of outgoing and incoming foreign transfers, the number of accounts opened during the year, the risks of cash transactions the bank deals with various clients, the complexity of accounts with correspondent banks, the volume of products related to gold or other precious metals, or any other products offered by the bank that are directly or indirectly linked to any type of unspecified financial business or profession. Through this monitoring, it is determined which of the bank's approved operations are high-risk and could be exploited as conduits for transactions suspected of money laundering and terrorist financing.

c. Service Delivery Channel Risks (Interface Risks):

- The bank must assess and document the risks of money laundering, terrorist financing, and other illicit activities posed by the digital transactions through which the business relationship is initiated, conducted, and continued. Furthermore, enhanced due diligence and ongoing monitoring procedures for the service delivery channel must be specific, appropriate, and proportionate to the apparent and potential risks posed by that channel.
- The bank must establish policies, procedures, systems, and regulations to address the risks of money laundering, terrorist financing, or other illicit activities posed by the various types of channels, interfaces, and technological developments through which the business relationship is initiated, conducted, and continued. These policies, procedures, and systems must include measures to prevent the misuse of technological developments in money laundering and terrorist financing operations, as well as to manage risks associated with the business relationship or non-face-to-face transactions.
- The bank must include in its procedures a method for classifying customers in relation to the service delivery channels through which the business relationship is initiated, conducted, and continued.

d. Risks Related to Geographic Areas

- The bank must assess and document the risks of involvement in money laundering, terrorist financing, and other illicit activities posed by the various geographic areas to which its customers are or may be affiliated. Such affiliation may be related to the customer's place of residence or business in foreign countries, and the source and destination of transactions conducted for their benefit. When identifying high-risk geographic areas, the bank may be guided by the following:

  - Countries subject to sanctions, transaction bans, or other similar measures from the United Nations.
  - Countries that do not have appropriate legislation or systems to combat money laundering and terrorist financing, or do not implement the Financial Action Task Force's recommendations, or do not implement them effectively.
  - Countries that finance or support terrorist activities.
  - Countries known for a high level of corruption or other illicit activities, such as drug trafficking, drug cultivation, arms smuggling, and others.

- The bank must have policies, procedures, systems and regulations to address the specific risks of money laundering, terrorist financing and other illegal activities posed by the various countries to which its clients are or may be affiliated.

First: It requires taking into account the locations of the customers with whom the bank deals who are from or reside in border areas, as well as the financial transactions carried out for customers in high-risk countries. Examples of this include:

- Nationality of the natural/legal customer.
- Country of residence of the natural/legal customer.
- Country of operation (i.e., the country in which natural or legal persons operate and conduct their business).
- Country of registration of the legal entity.
- Customers of branches located in border areas.

Second: Countries and states identified by the Financial Action Task Force (FATF) or similar regional organizations as having strategic deficiencies in their AML/CFT systems (blacklist).

Third: Countries and states that lack adequate AML/CFT systems or do not adequately implement FATF recommendations and are subject to increased monitoring by the FATF (grey list).

To assess the effectiveness of AML/CFT systems in other countries, the bank must consider the following three factors, at a minimum:

- Legal framework in these countries.
- Imposition of sanctions and supervision.
- International cooperation.

Article 3: The Principle of Notification (Reporting)

Banks must establish an effective mechanism for internal and external reporting whenever a suspected money laundering or terrorist financing transaction is detected, including the following:

1. The bank must develop effective policies, procedures, and regulations for reporting all suspected money laundering or terrorist financing transactions, including attempts to conduct such transactions, to the Anti-Money Laundering and Terrorist Financing Office, regardless of the size of the transaction. These policies and procedures must enable the bank to comply with the law, its implementing regulations, and these regulations regarding the prompt submission of reports on suspicious transactions to the Office, as well as effective cooperation with law enforcement agencies.
2. The notification must include a detailed explanation of the reasons and justifications on which the bank based its determination that the transaction is suspicious, as well as the facts or circumstances on which the bank based its suspicion.
3. The notification must be made in accordance with the form prepared by the Anti-Money Laundering and Terrorist Financing Office for this purpose, which was circulated by the Office to banks, along with instructions for its completion. The notification must also include all data and copies of documents related to the suspected transaction, taking into account compliance with the instructions for completing the aforementioned form.

4. The bank must ensure that it has effective policies and procedures for internal reporting of all suspected money laundering and terrorist financing transactions. These policies and procedures enable the bank to comply with the law, its implementing regulations, and these regulations, and allow for the prompt submission of internal reports on suspected transactions to the bank's Anti-Money Laundering Department official.
5. The bank must ensure that all its officials and employees have direct access to the Anti-Money Laundering Department official and that the reporting mechanism between them is straightforward. Furthermore, all officials and employees are obligated to report any suspicious transaction when they have reasonable grounds to suspect or suspect that funds being transferred through the bank are the proceeds of criminal or illegal activity, are linked to terrorist financing, or are intended to be used to carry out terrorist acts or are being used by a terrorist organization.
6. The bank's officials and employees must promptly submit an internal report on the suspected transaction to the Anti-Money Laundering Department official. This report must include all details of the customer's subsequent transactions. The Anti-Money Laundering Department official must document the report appropriately and provide the employee with a written acknowledgment of the report. The employee must also be alerted to the provisions relating to confidentiality and to disclosure or insinuation to the customer. The Anti-Money Laundering Department official must also review this report in light of all information available to the bank, decide whether the transaction is suspicious, and provide the employee with a written notification.
7. It is prohibited to disclose to the customer, the beneficiary, or to anyone other than the authorities and entities entrusted with implementing the provisions of the law and regulations any reporting procedures taken regarding financial transactions suspected of involving money laundering or terrorist financing, or any related data.
8. Bank employees are trained on the suspicious indicators for transactions that may involve money laundering or terrorist financing, including the basic suspicious indicators for money laundering and terrorist financing.
9. Officials in the Money Laundering and Terrorism Financing Reporting Department must educate and raise awareness among all employees of the financial institution regarding reporting transactions suspected of involving money laundering and terrorist financing. They must clarify to them that anyone who reports such transactions is protected and will not be subject to any legal action, based on the provisions of Article 48 of the Anti-Money Laundering and Terrorism Financing Law No. 39 of 2015, which stipulates that "no person who reports in good faith any of the suspected transactions subject to the provisions of this law or provides information or data about them, even if it is proven to be false, shall be criminally or disciplinary liable."
10. Based on the content of Article 12, Paragraph (Fifth/A) of the Anti-Money Laundering and Terrorist Financing Law No. 39 of 2015, which stipulates that the Office shall be immediately informed of any operation suspected of involving money laundering or terrorist financing, whether this operation has taken place or not, and in accordance with the reporting form prepared by the Office for this purpose. All employees working within the financial institution must act in accordance with the provisions of the aforementioned article and inform the Anti-Money Laundering and Terrorist Financing Office of any suspicious operation, whether it has taken place or not, so that the Office can take the necessary measures.
11. The financial institution's senior management must ensure that all employees involved in combating money laundering and terrorist financing report any suspicious transactions in accordance with the reporting procedures approved by the Anti-Money Laundering Office, and the risk profile and penalties for employees failing to report suspicious transactions, as stated in Article 39 (Second/A) of the aforementioned Anti-Money Laundering and Terrorist Financing Law.

Article 4: The Principle of Effective Investigation and Screening and Continuous Training of Employees

Banks must establish screening procedures to ensure high standards of competency when appointing or hiring officials or employees, and must also establish an ongoing training program for their officials and employees on anti-money laundering and counter-terrorist financing methods, as follows:

1. The bank must develop appropriate and ongoing training plans and programs, at least annually, to train its officials and employees on anti-money laundering and counter-terrorist financing.
2. The bank's training program must include ongoing training to ensure that its officials and employees maintain their knowledge, skills, and abilities to enhance their proficiency in strictly complying with the established rules and regulations for combating money laundering and terrorist financing. It must also keep them informed of new developments related to the methods and general trends of money laundering and terrorist financing operations, their counter-terrorism systems, and local, regional, and global developments in this regard.
3. The bank must conduct a periodic review of its training needs and examine these needs. This review should consider existing expertise, skills, and capabilities, the required functions and roles, the bank's size, the bank's risk classification, the results of prior training, and the identified needs. The Board of Directors must also take the results of each review into account.
4. These programs should be planned and implemented in coordination between banks, the Anti-Money Laundering Office, and the Central Bank of Iraq, taking into account the following:

    a. Training must be comprehensive for bank units, officials, and employees.
    b. To implement training programs, seek assistance from specialized institutes established for this purpose, or those whose objectives include training in the field of combating money laundering and terrorist financing, whether local or international, while benefiting from local and international expertise in this regard.
    c. To coordinate with the Compliance Officer regarding the selection of employees nominated to attend training programs in this field.

Chapter 3: Responsibilities of the Board of Directors, the Head of the Money Laundering Reporting Department, and External Auditors

Article 1: Responsibilities of the Board of Directors

The Board of Directors and senior executive management of banks must ensure that the bank's internal policies, regulations, procedures, and systems are consistent with the Anti-Money Laundering and Counter-Terrorism Financing Law, its Executive Regulations, and these regulations by doing the following:

1. Establishing appropriate written internal policies, procedures, and regulations for the proper implementation of the Law, its Executive Regulations, and the instructions issued by the Central Bank of Iraq related to combating money laundering and terrorist financing.
2. The Board of Directors shall be primarily responsible for the effectiveness of internal policies, procedures, systems, and regulations related to combating money laundering and terrorist financing, and for approving policies and procedures related to combating money laundering and terrorist financing.
3. Conducting due diligence and investigations and applying the best standards when appointing or hiring officials or employees within the bank.
4. Providing an appropriate and ongoing training program for officials and employees on methods and techniques for combating money laundering and terrorist financing.
5. Establishing a Money Laundering Reporting Department to monitor all branches, in implementation of Article 14 of the Anti-Money Laundering Law No. 39 of 2015.
6. Ensuring that the Money Laundering and Terrorist Financing Reporting Department is linked to the Board through the Audit Committee of the Board of Directors, based on the Corporate Governance Manual issued by this bank. This department is responsible for implementing policies and processes related to Know Your Customer (KYC) procedures, and the duties and responsibilities resulting therefrom, including the department's preparation of periodic reports on its activities.
7. Appointing a Money Laundering Reporting Department official and his deputy within the bank and ensuring that they are granted full powers and independence.
8. The Board of Directors must ensure the provision of the necessary technical resources from reliable and high-quality sources, including, but not limited to, the AML/CFT system, and the search and investigation systems that provide interconnected international lists and the overall banking system, ensuring the necessary effectiveness in detecting unusual transactions.
9. Establish an independent internal audit function with sufficient resources to test compliance with AML/CFT policies, procedures, systems, and regulations.
10. The bank must have specific risk management methodologies in place with regard to AML/CFT.
11. The bank must document its risk management policies and methodologies.
12. Take the necessary measures to ensure that AML/CFT risks are considered when implementing these measures in daily transactions, developing new products, and accepting new customers.
13. Review AML/CFT procedures for existing customers.
14. Review the monthly and quarterly reports of the AML/CFT Reporting Department through the Audit Committee and the Board of Directors.
15. The Board must: Through the Audit Committee and the bank's supervisory departments or divisions, the bank shall ensure that the bank implements customer due diligence measures in

16. accordance with Anti-Money Laundering and Terrorism Financing Law No. 39 of 2015 and the instructions issued pursuant thereto.
17. The Board shall ensure that the bank retains the following records, documents, and papers for a period of five years from the date of termination of the relationship with the customer or from the date of closing the account or executing a transaction for a casual customer, whichever is longer, and shall ensure that they are made available to the competent authorities as quickly as possible. These records shall include, at a minimum, the following:
    a. Copies of all records obtained through the due diligence process in verifying transactions, including documents proving the identities of actual beneficiary customers, accounting files, and business correspondence.
    b. All records and transactions, both those actually executed and those attempted, provided that these records are sufficiently detailed to allow for a representation of the steps of each transaction.

18. Preparing, implementing, and adopting programs to prevent money laundering and terrorist financing, including:
    a. Conducting an assessment of the money laundering and terrorist financing risks to which the organization is exposed, including identifying, assessing, and understanding these risks, taking effective measures to mitigate them, and providing this assessment to regulatory authorities.
    b. Adopting policies, procedures, and internal regulations appropriate to the implementation of obligations imposed in the field of combating money laundering and terrorist financing, thus mitigating the assessed risks.
    c. Establishing and applying appropriate integrity standards when selecting employees.
    d. Providing ongoing training for officials and employees working in the field of combating money laundering and terrorist financing, and allocating the necessary material and financial resources to them to ensure their capabilities are enhanced in understanding the risks of money laundering and terrorist financing, identifying unusual or suspicious transactions and behaviors, how to deal with them, and effectively implementing the necessary measures.
    e. Conducting an independent audit to test the effectiveness of policies and procedures and their implementation.
    f. The system must be efficient and effective in measuring risks related to customers, the nature of their business, and the customer's geographical location, using the latest methods approved in this field.

Article 2: Director (Responsible) of the Money Laundering and Terrorist Financing Reporting Department

The Director responsible for compliance at the bank shall be responsible for the Money Laundering and Terrorist Financing Reporting Department. A replacement shall be designated during their absence, and the Anti-Money Laundering Office and this bank shall be notified in the event of any change.

1. Regulations for the Appointment of the Director of the Money Laundering Reporting Department and their Assistant

a. The Director of the Money Laundering Reporting Department and their Assistant shall not be less than 30 years of age and shall be exclusively Iraqi nationals.
b. The Director of the Money Laundering Reporting Department and their Assistant shall hold an undergraduate university degree in law, financial management, public administration, accounting, financial and banking sciences, economics, or statistics. The educational attainment of the Assistant Director of the Money Laundering Reporting Department may be a diploma in the aforementioned specializations.
c. The Director of the Money Laundering Reporting Department and his assistant must have passed several courses in the field of combating money laundering inside or outside Iraq, not less than 50 training hours for the Director and 75 training hours for the assistant, and they must obtain the Certified Specialist in Combating Money Laundering (ACAMS) certificate or the Certified Specialist in International Bans and Sanctions (CGSS) or the Certified Specialist in Combating Financial Crime (CFCS) certificate, provided that the bank undertakes to include them in international training courses in the field of combating money laundering within one year from the date of their appointment, otherwise the approval of their appointment will be cancelled.
d. The Director of the Money Laundering and Terrorist Financing Reporting Department must have at least five years of banking experience and good command of the English language, and his/her assistant must have at least three years of banking experience and practice.
e. They must be exclusively Iraqi nationals, residing in Iraq, with a permanent and known address, and dedicated to the position. They must not be employees of a bank, company, or other financial institution.
f. They must not have been convicted of a felony or misdemeanor involving moral turpitude, and no decision must have been issued against them by a competent authority that would impair their ability to perform any leadership position (bank or company).
g. The appointment of the Director of the Money Laundering and Terrorist Financing Reporting Department must be approved by the Central Bank of Iraq after passing the examination. They may not be dismissed except with the approval of the Central Bank of Iraq. The Central Bank of Iraq may also request the dismissal of their services if they prove unable to perform this task or for any other reasons the Bank deems appropriate.

The following criteria shall be taken into account when determining the responsible manager and his replacement in his absence. He shall have the guarantees, powers, and duties set forth below:

1. Guarantees and powers of the manager responsible for the Money Laundering/Terrorist Financing Reporting Department: The manager responsible for this department must be independent in performing his duties and be provided with the means necessary to carry out these duties in a manner that achieves its purpose. This requires the following:

    a. Not assigning him any tasks that conflict with his duties after he becomes the manager responsible for the Money Laundering and Terrorist Financing Reporting Department.
    b. He shall have the right to obtain all information and review all records or documents he deems necessary to carry out his duties in examining unusual transactions reports and suspicious transactions reports submitted to him, and to contact any bank employees necessary to carry out these duties.

c. The Bank shall have the right to submit reports to the Board of Directors through its connection to the Audit Committee, which is affiliated with the Board of Directors and the Bank's senior management, through the Bank's organizational structure. This will help increase the efficiency and effectiveness of the AML/CFT systems and the commitment of employees to them.
d. The Bank shall ensure complete confidentiality regarding all procedures for receiving unusual transaction reports and suspicious transaction reports, as well as the examination and notification thereof to the Anti-Money Laundering Office.
e. Coordinate and cooperate with the Bank's Compliance Department, Risk Management Department, and Information Technology Department regarding the implementation of AML/CFT scenarios in a manner that ensures optimal implementation of the requirements of the Central Bank of Iraq and the Anti-Money Laundering and Terrorism Financing Office, and make the necessary additions and amendments upon issuance of instructions from regulatory authorities.

2. Duties of the Director Responsible for the Money Laundering/Terrorist Financing Reporting Department: The duties of the Director Responsible for the Money Laundering/Terrorist Financing Reporting Department in each bank are determined according to the bank's size, resources, and applicable systems. In general, the Director must be assigned the following tasks:

a. Examining unusual transactions that the bank's internal systems allow, and examining suspicious transactions submitted to him by bank employees, accompanied by justifications, or submitted to him by any other party.
b. Notifying the Anti-Money Laundering Office of transactions involving suspected money laundering or terrorist financing, in accordance with applicable forms.
c. Making decisions regarding the filing of transactions that he determines are not suspicious. The decision must include the reasons for filing.
d. Proposing any necessary developments and updates to the bank's policy in the field of combating money laundering and terrorist financing, as well as the systems and procedures followed by the bank in this field, with the aim of increasing their effectiveness and efficiency and keeping pace with local and global developments.
e. General supervision, both in the office and in the field, of the commitment of all bank branches to implementing the provisions of the laws, regulatory regulations and internal regulations of the bank in the field of combating money laundering and terrorist financing
f. Cooperate and coordinate with the relevant department at the bank regarding the development of training plans for bank employees in the field of combating money laundering and terrorist financing, propose the necessary training programs to implement these plans, and follow up on their implementation.
g. Conduct field visits and on-site inspections of high-risk customers dealing with the bank.
h. Cooperate with the bank's Compliance Department, Risk Department, and the Director of the Money Laundering and Terrorist Financing Reporting Department on all matters related to the money laundering risks to which the bank may be exposed, by preparing joint reports or plans in this regard.
i. Ensure that the number of department employees is proportionate to the volume of business in the bank's branches and supervise liaison staff within the bank's branches.
j. The Director of the Money Laundering and Terrorist Financing Reporting Department monitors and audits the monthly reports prepared by the liaison staff in the Money

Laundering and Terrorist Financing Reporting Department at all bank branches. These reports must include the cases reported and the latest actions observed during the month and be made available upon request by inspection bodies.

k. Submit quarterly reports to the Board of Directors, through the Audit Committee, on the efforts undertaken during the reporting period regarding unusual and suspicious transactions, and the actions taken in this regard. A copy of the reports is kept in the bank's files, subject to review by the Central Bank of Iraq's field inspection committees that visit the bank.
l. Verify the validity of all account opening procedures and supporting documents for the activities undertaken by companies and individuals, such as (official documents and identification papers, articles of association, work and professional licenses, import invoices, etc.), for example.
m. Analyze customer financial statements and ensure their consistency with the volume of transactions and account activity.
n. Update the Know Your Customer (KYC) form periodically, no less than once a year.
o. Conduct research, investigation, and examination procedures, and apply the best standards when appointing or hiring officials or employees within the financial institution.
p. Preparing a policy for correspondent banks, in coordination with the International Department, that includes the names of the correspondent banks with which the bank deals and their ratings based on the ratings approved by international rating agencies. It also includes the risks surrounding these banks in terms of money laundering and terrorist financing risks, and the due diligence measures taken with them.
q. Preparing a semi-annual report on the bank's anti-money laundering and counter-terrorism financing activities and presenting it to the Audit Committee, and subsequently to the Board of Directors for their comments and action. This report is then sent to the relevant authority at the bank, along with a copy to the Anti-Money Laundering and Counter-Terrorism Financing Office, along with the comments and decisions of the bank's Board of Directors.
r. Preparing an annual report on the bank's self-assessment of money laundering and terrorist financing risks, in coordination with the Risk Management, Compliance, and Internal Audit departments.
s. Preparing quarterly reports on the bank's anti-money laundering and counter-terrorism financing (AML/CFT) activity, keeping them in the department's records, and submitting them to field inspection committees that visit the bank. This report should include, at a minimum, the following:

    i. The efforts made during the reporting period regarding unusual and suspicious transactions, and the actions taken in this regard.
    ii. The weaknesses identified by the periodic review of the bank's AML/CFT systems and procedures, and proposals for addressing them, including reports made available through the bank's internal systems on unusual transactions.
    iii. The number of alerts on the bank's AML/CFT systems that were followed up, and whether they would have required reporting, and the reason for doing so.
    iv. The amendments made to the bank's policies, internal systems, or procedures in the field of AML/CFT during the reporting period.
    v. A statement of the extent of compliance with the implementation of the plans developed during the reporting period for general office and field supervision of the bank's various branches to verify their compliance with the provisions of the laws, regulatory regulations, and internal regulations in the field of combating money laundering and terrorist financing.

vi. Presentation of the plan developed for general office and field supervision of the bank's branches during the reporting period.
vii. A detailed statement of the training programs held for the bank's employees in the field of combating money laundering and terrorist financing during the aforementioned period.

Article 3: Additional Requirements of External Auditors

1- Additional Special Reports

a. The auditors shall provide the Central Bank of Iraq with a letter of observations, whether or not it has been responded to by the bank's management.
b. A report on violations and transgressions of the laws and instructions regulating banking operations and the bank's compliance with the approved accounting rules and principles and the instructions of the Central Bank of Iraq, primarily with regard to the following:
   - Credit concentrations and the bank's compliance with the maximum limits of credit facility risks.
   - Dealing with related parties (members of the board of directors and related institutions, major shareholders - the bank's subsidiaries) and the bank's compliance with the maximum limits.
   - Exposure to foreign exchange risks.
   - The bank's accurate calculation of the capital adequacy ratio, the legal liquidity ratio prescribed by the bank, the net stable funding ratio (NSFR), the liquidity coverage ratio (LCR), and cash maturities according to the maturity scale, in accordance with the instructions.

c. Reviewing the money laundering and terrorist financing systems. The digital system adopted by the bank to combat money laundering and terrorist financing must be reviewed. This system must include, at a minimum:
   - The digital system includes the minimum required scenarios.
   - The digital system includes periodic and automatic updates of blacklists specified by the Anti-Money Laundering and Terrorist Financing Office and the Central Bank of Iraq.
   - The bank's digital system classifies customers based on their risk level.
   - The extent to which the system is used to monitor the bank's customers' compliance and compare the volume of transactions reviewed by the system to the bank's total operations.

d. A special report on debt classification, clearly stating the adequacy or inadequacy of provisions for classified debts, along with an estimate of the provisions to be established, if necessary. If no explicit opinion is expressed in this regard, it can be concluded that the provisions established by the bank are sufficient, in the opinion of the external auditors, in accordance with the instructions of the Central Bank of Iraq in this regard.
e. The extent of the bank's application and compliance with International Financial Reporting Standards (IFRS) and International Accounting Standards (IAS) through the presentation of the interim and final financial statements.

f. The number of meetings held by the auditor with both the internal auditor and the board of directors, and the outcomes of these meetings, based on the corporate governance manual issued by the bank.
g. A report on the bank's compliance with internal control systems, the external auditor's opinion and recommendations, and management's view of weaknesses.
h. The external auditor must pay particular attention to the bank's compliance with the required internal control procedures, including, for example:
    - Administrative organization and segregation of responsibilities and authorities.
    - Organization of loan and facility files.
    - The work of the internal audit department.
    - Correspondent bank account reconciliation statements.
    - Revenue and expense accounts.
    - Regular accounts (contingent liabilities - off-balance sheet items).

i. A report on the bank's compliance with the anti-money laundering and counter-terrorism financing system, explaining the bank's mechanism for operating under the "know your customer" principle.
j. A report on digital banking transactions (number of ATMs and points of sale, and any problems faced by these transactions, if any).
k. A report on the activity of the bank's compliance monitor and the extent to which he monitors the compliance of all bank departments and branches with the regulations and instructions issued by the Central Bank of Iraq.
l. A verification of the efficiency and validity of the bank's control and risk systems and their suitability for the volume of business carried out by the bank.
m. A disclosure of any bonuses granted by the bank to members of the board of directors or any other bonuses granted to executive management during the period of preparing the financial reports and the reason behind granting these bonuses.
n. The bank's percentage of shareholding in any affiliated or subsidiary companies, the price of the bank's shares listed on the Iraq Stock Exchange, and the estimated fluctuations in the share price during the fiscal year.

The auditor must exercise special professional care regarding the following matters:

- Verifying the bank's account balances with banks and whether they are truly liquid, free funds, and not bound by any obligations. Furthermore, ensuring that the reconciliations do not show any suspended amounts, with the necessity of indicating the size of the balances. The amounts held by any bank, and the purpose of their binding and freezing, as well as any outstanding amounts in the reconciliations, should be clarified, along with an estimate of the potential losses that may result from these amounts, if any.
- Verifying the accuracy of the bank's credit and debit account balances with the head office and sister and affiliated financial institutions, detailing the amount of these amounts in a separate item. It is necessary to indicate the amount of the restricted amounts, clarify the purpose of their binding and freezing, and highlight any outstanding amounts, along with an estimate of the potential losses that may result from these amounts, if any.
- The adequacy of the internal control and accounting systems, and the extent of the bank's compliance with them.
- The method of maintaining records and documents and how they are prepared.

- The adequacy of the bank's management and its performance with regard to protecting the bank's funds and the funds of its depositors.
- Deficiencies in the bank's activities and the recommendations of the auditor to the Board of Directors
- The extent to which the data sent to the Central Bank of Iraq conforms to the content of the records, books, and systems, and to the instructions of the Central Bank of Iraq.
- The extent to which the bank applies international financial disclosure standards, including International Standard No. 9, and the adequacy of provisions allocated in accordance with this standard.
- The extent to which the bank has taken adequate measures to combat money laundering and terrorist financing, and whether or not these measures are being implemented in accordance with the regulations and directives issued by the Central Bank of Iraq under Paragraph 1/d of Article 47 of Banking Law No. 94 of 2004.
- Expressing an opinion on the bank's ability to fulfill its obligations to depositors in terms of solvency and liquidity during the coming year.
- Disclosing in detail the profits and sales of the foreign currency buying and selling window, comparing them with the exchange rate approved by the bank and the exchange rate in the parallel market, and calculating the average dollar selling price at banks during the fiscal year relative to the volume of purchases from the bank.
- Reviewing the credit files of a sufficient sample of no less than the 20 largest borrowers and expressing an opinion on their solvency, the collateral provided, and their compliance with the regulations and instructions issued by the bank.
- Reviewing bank balances with foreign correspondent banks and ensuring that these balances do not exceed the legal ratios set by the bank.
- Ensuring that no balances are held with correspondent banks rated lower than (B-) by an accredited credit rating agency. Otherwise, provisions are made to cover any balances with banks rated lower than (B-).
- Expressing an opinion on the extent of the bank's and board's commitment to implementing the corporate governance instructions issued by the bank regarding disclosure and transparency practices.
- The bank's commitment to implementing the quantitative and qualitative requirements contained in the environmental, social, and corporate governance elements approved by the Central Bank of Iraq.
- Reviewing correspondence from the Central Bank of Iraq related to business oversight and the results of the bank's off-site audit, and expressing an opinion on the bank's compliance with the Central Bank of Iraq's observations and recommendations related to business oversight and the results of the off-site audit.
- Verify the correctness of the calculation and recording of interest received and paid on their due dates and ensure that they are transferred to the profit and loss account in the currency on the due date, with respect to the bank's dealings with other banks, particularly the head office, branches, and affiliated banks and financial institutions. It is necessary to point out any procedures that violate the accounting rules and banking practices followed in this regard.
- Verify and report the accuracy of the balances of contingent liabilities and settlement accounts, including the head office and branch accounts, and ensure that they do not include any items outstanding for an unreasonable period or any abnormal or non-temporary items that conceal the bank's exposure to foreign exchange risks or result in any losses to the bank's financial position.

2- Other matters that must be adhered to

a. In the event of the resignation or dismissal of the external auditor, he must provide the Central Bank with an explanatory letter explaining the reasons and circumstances of the resignation or dismissal.
b. The auditors must immediately inform the Central Bank of Iraq of:
   - Any difficulties or pressures they encounter in the performance of their duties.
   - Any violations that require immediate reporting under laws, regulations, circulars, and periodicals, and those that the auditor believes his professional duty requires him to report to the Central Bank of Iraq.

c. The auditor must adhere to international auditing standards and the instructions of the Central Bank of Iraq, while balancing the available human, material, and technical capabilities, particularly with regard to the number of partners, their competence, and the experience gained from their work in auditing bank data, as well as the number and size of contracted banks.
d. The auditor must evaluate the automated system, the degree of security, and the work performed by the competent department and express an explicit opinion thereon.

3- The auditor must prepare the aforementioned reports and attach them to the annual budget or submit them individually to the Central Bank of Iraq in one batch on the specified date. In exceptional cases where the auditor is unable to adhere to the deadline for submitting the reports, he must submit a request for approval from the Central Bank of Iraq to extend the reporting deadline, explaining the reasons and the required extension period.

Article 4 - Compliance Controller

Legal Basis

Paragraph (First) of Instructions No. 4 of 2010 to Facilitate the Implementation of Banking Law No. 94 of 2004 stipulates The Board of Directors of an authorized bank shall appoint a compliance controller for the bank, subject to the following conditions:

1. The employee must have legal capacity and be a suitable and competent person.
2. The employee must have the banking expertise and experience required for banking operations.
3. The employee must not be an administrative person, an employee of another bank, or an authorized manager of another bank.
4. The employee must be a resident of Iraq and be dedicated to the bank's work.

Duties of the Compliance Controller

It is essential to define the duties and responsibilities of the Compliance Controller, and the bank's senior management must fully and in writing clarify this. This must also clarify the relationship of the Compliance Controller with senior management and the various departments within the bank. The Compliance Controller's role generally includes the following duties:

1. Reviewing policies, procedures, and senior management decisions related to the bank's activities, determining their consistency with relevant laws, regulations, and regulatory instructions, and

providing comments on them. The Compliance Controller attends all Board of Directors meetings as an observer.

2. Proposing the necessary policies and procedures for new banking operations or updating previous policies and procedures for existing banking operations, based on the requirements of the banking activity, the development of its business, and its relationships. These policies and procedures must be approved by the bank's Board of Directors.
3. Preparing the department's policies and procedures on an annual basis, presenting them to the Board of Directors for approval and submitting them to the Central Bank of Iraq for review.
4. Review the procedures followed by the bank's various departments and divisions, ensuring their consistency with relevant laws and regulations, assessing the adequacy of internal procedures and directives, monitoring deviations, and submitting proposals for addressing and improving them.
5. Submit semi-annual reports to the Central Bank of Iraq, with a copy to the Board of Directors, on identified deviations, including suggestions and necessary corrective actions to avoid recurrence in the future. A copy of these reports is kept in the bank's files, subject to review by the Central Bank of Iraq's field inspection committees that visit the bank.
6. Submit monthly reports to the senior management and the Audit Committee, based on the Environmental, Social, and Corporate Governance Standards Manual issued by the bank, including any identified deviations and suggestions for remediation. The report also monitors the implementation of all laws, instructions, and circulars issued by the Central Bank of Iraq through the daily operations of all departments. A copy of these reports is kept in the bank's records for review by the Central Bank of Iraq's field inspection committees upon request.
7. The Compliance Officer assesses the bank's compliance with relevant legal requirements in its operations. He also ensures the validity of applicable policies and procedures and works to avoid any potential errors or legal violations.
8. Proposes training courses on established policies and procedures, emphasizing the need for compliance from employees in general, and new employees in particular.
9. Familiarizes himself with all laws, regulations, and instructions related to banking activity. This should include requirements that may not be directly related to banking activity and operations. The bank's legal department can provide significant support in developing this task.
10. Establishes a digital compliance library that includes all laws, regulations, and systems related to banking activity and updates it periodically.
11. Preparing a list of banking products, services, and business areas. This will help identify all business areas not previously covered, in consultation with all heads of the various business sectors within the bank.
12. Regulating banking activities, products, and services, along with their corresponding legal requirements and related regulations. This can be achieved by first identifying the applicable law and then identifying the banking businesses and services that fall under this law.
13. Distributing compliance-related information to those responsible for implementation. This helps review formulas and procedures when changes are required, defines procedures related to new products, assists in resolving problems, and follows up on corrective actions.

Many compliance auditors, according to global experience, organize their work based on the results of recent inspections covered by inspectors. This is impractical, as inspectors often change their focus from one inspection to the next. Therefore, the compliance auditor should consider these results as interim priorities, not as a basis for structuring their daily work.

Qualifications Required for the Compliance Controller

The Compliance Controller is the person responsible for monitoring compliance with the policies and procedures established by the laws and regulations issued by the Central Bank and the decisions of the Bank's Board of Directors. Therefore, their qualifications must comply with the specifications stipulated in the Banking Law, which are mentioned in the legal basis for these instructions. In addition, the following must be met:

- The Compliance Controller and their assistant must be at least 30 years old.
- The Compliance Controller and their assistant must hold an undergraduate university degree in law, financial management, public administration, accounting, financial and banking sciences, economics, or statistics.
- They must have sufficient experience in banking work in all fields, with at least five years for the manager and 75 hours of training, and three years for the assistant and 75 hours of training, in addition to a good command of the English language.
- They must have a comprehensive knowledge and understanding of the laws, regulations, and instructions issued by the Central Bank and laws indirectly related to financial and banking operations. They do not need to be legally qualified. He or she must have knowledge of international banking services that can be applied in Iraq, in accordance with the requirements of the development of banking activity in Iraq and in harmony with the requirements of the evolving Iraqi economy.
- The appointment of the Compliance Controller shall be subject to the approval of the Central Bank of Iraq after passing the examination. The Compliance Controller may only be dismissed with the approval of the Central Bank of Iraq. The Central Bank of Iraq may also dismiss the Compliance Controller if it is determined that he or she is unable to perform his or her duties.
- The Compliance Controller must have completed specialized training courses in the field of compliance. Both the Manager and the Assistant Manager must hold the Certified Compliance Manager (GCI) or the International Advanced Certificate in Compliance (ICA). For Islamic banks, the Compliance Controller must hold the Certified Islamic Specialist in Governance and Compliance (CIGC) certificate issued by the General Council for Islamic Banks. The bank must undertake to provide them with international training courses in the field of compliance within one year of their appointment; otherwise, their appointment will be revoked.

Job Description for the Compliance Controller

It is essential to develop a comprehensive, written job description for the Compliance Controller, including:

1. Clarification of the general responsibilities, areas of work, and the banking products and services included.
2. Develop a list of tasks to be performed by the compliance officer in carrying out his duties, with instructions issued later.
3. Define his powers and relationship with other departments within the bank. Preferably, he should be at the level of expert, assistant general manager, or authorized assistant manager, and participate in board meetings as an observer.
4. Assist in resolving problems, following up on corrective actions, and training employees.
5. Work with auditors and inspectors to help develop appropriate control measures to avoid future problems.

To be more effective, the compliance officer needs various sources of information. The most important of these sources is the library he or she creates, which must contain comprehensive information on the laws, regulations, and banking products for which the compliance officer is responsible. At the same time, and no less important than the library, it is important to establish strong working relationships within the bank, preferably by forming a compliance oversight committee headed by the compliance officer. This process will help in two ways:

a. Obtaining the necessary information from various sources.
b. Forming a core group whose members can identify problems and issues for resolution, propose proposals related to the implementation of regulations and their impact on the bank's operations, and formulate appropriate opinions for conveying them to the issuing authorities.

Compliance Department Requirements

1. The bank's compliance department must be functionally, administratively, and technically independent. The concept of independence is based on four elements related to this independence:

   - The compliance department must have a formal and clear status within the bank.
   - The compliance officer must be appointed and assume overall responsibility for coordinating the bank's compliance risks.
   - Compliance Department employees, particularly the Compliance Controller, should not be assigned positions that could create a conflict of interest between their compliance responsibilities and the duties of their assigned position.
   - Compliance Department employees should have access to information and staff to carry out their responsibilities.

2. The bank's Compliance Department should have sufficient and appropriate financial and human resources. These resources should be provided to the Compliance function to ensure the effective functioning of the bank's compliance risk management. Compliance department employees should possess the necessary qualifications, experience, professional and personal characteristics, and be well-versed in applicable laws and regulations.
3. Compliance personnel should possess the necessary professional skills to keep abreast of developments, compliance procedures, rules, and standards through regular, structured educational and training courses.
4. The bank's compliance activity responsibilities should aim to assist executive management in effectively managing the compliance risks faced by the bank. The compliance activity responsibilities are defined in accordance with these regulations. If some of these responsibilities are performed by employees working in different departments, responsibilities should be clearly distributed among each department. These responsibilities include the following:

   - Advice.
   - Guidance and education.
   - Identifying, measuring, and assessing compliance risks.
   - Monitoring, testing, and reporting risks.
   - Legal responsibilities, liaison, and coordination with relevant external parties, regulators, standard setters, and external experts.
   - Fulfilling the responsibilities specified in the bank's compliance policy.

5. The bank's executive management must engage compliance department employees in professional development courses and allocate the necessary funds to keep abreast of recent developments in the field of compliance. When the Central Bank of Iraq evaluates the performance of a bank's compliance department, it will take into account that these courses constitute an important part of the bank's business.
6. Compliance is a core activity in risk management within the bank. Specific compliance tasks may be outsourced. These tasks and resources must remain under the effective oversight of the Compliance Department Manager. Both the bank and the company providing the outsourced service remain accountable to the bank.

Compliance Controller's Activities in Combating Money Laundering:

1. The compliance controller must prepare a periodic report at least once every six months on the bank's anti-money laundering activity and submit this report to the bank, accompanied by the comments and decisions of the financial institution's board of directors. This report must include, at a minimum, the following:
2. The efforts made during the reporting period regarding unusual and suspicious transactions, and the actions taken in this regard.
3. The weaknesses identified in the periodic review of the institution's anti-money laundering systems and procedures, and proposals for addressing them, including reports made available by the financial institution's internal systems on unusual transactions.
4. Any amendments made to the financial institution's policies, internal systems, or procedures in the field of combating money laundering and terrorist financing during the reporting period.
5. A statement of the extent of compliance with the plans developed during the reporting period for general office and field supervision of the financial institution's various branches to verify their compliance with the provisions of laws, regulatory regulations, and internal systems in the field of combating money laundering.
6. A presentation of the plan developed for general office and field supervision of the financial institution's branches during the reporting period.
7. A detailed statement of the training programs conducted for the financial institution's employees in the field of anti-money laundering during the period covered by the report.
8. The means provided by the bank to perform its duties independently.
9. The results of its review of the bank's anti-money laundering systems and the extent of employees' compliance with these systems.
10. The role performed by the bank's Board of Directors in overseeing the anti-money laundering systems and addressing any deficiencies.

Compliance Controller Job Description

Compliance control is an independent function within each bank that ensures the bank's compliance in its daily banking operations with the requirements of the relevant laws and regulations issued by the Central Bank, as well as with policies and procedures, in accordance with the relevant laws and instructions. This is done in cooperation with the bank's executive departments to ensure the validity of these policies and procedures and to avoid errors and violations that could expose the bank to various risks. Compliance controllers must send their reports to the bank and copies thereof to their respective departments. These reports may not be submitted through their bank's management.

Article 5: Risk Management

The importance of risk management lies in understanding the potential positive and negative aspects of all banking services that may affect the institution. It increases the likelihood of success and reduces both the likelihood of failure and uncertainty regarding the achievement of the institution's overall objectives.

First: The most important procedures that a bank must adhere to in the area of risk management

1. Establish a risk management department.
2. Prepare a general policy for the bank that includes, at a minimum, defining risk ceilings for all types of risks.
3. Clearly define risk management procedures that are consistent with the complexity and degree of its operations.
4. Identify the types of financial instruments and transactions permitted and accurately determine the risk level for these instruments and investment portfolios.
5. Periodically review the policies and procedures in place and work to amend them to suit the bank's activity and risks.
6. Identify the risks resulting from the use of new financial instruments and activities before engaging in them.
7. Develop operational procedures and internal regulations for each new financial instrument or activity before engaging in them.
8. This department shall be under the direct supervision of the bank's Board of Directors or the bank's Senior Risk Management Committee.
9. Taking the necessary measures to improve risk management systems in line with the observations and suggestions of the internal auditor, the bank's auditor, and the Central Bank.
10. Recommending the abandonment of activities that pose risks to the bank that the bank is unable to address.
11. Determining limits for the risks the bank can tolerate, provided this does not affect the adequacy of the bank's own funds or the results of its operations.
12. Continuously cooperating with the bank's risk management authorities to review all bank activities, assess the risks they may pose, ensure that the bank's internal control system is capable of monitoring these risks, and determine the necessary measures to manage and mitigate them.
13. Preparing risk reports and submitting them to the Board of Directors.
14. Coordinating the activities of the various functions that provide advice on risk management within the institution.
15. Building a cultural awareness of risk within the institution, including appropriate education and ongoing training.

Second: Risk Management Steps

1. Risk Identification: For a bank to be able to manage risks, it must first identify them. Every product or service offered by the bank involves a number of risks, including interest rate risk, lending risk, liquidity risk, and operational risk.
2. Risk Measurement: The second step after identifying risks is measuring them. Each type of risk must be considered from three dimensions (magnitude, duration, and likelihood of occurrence). Time is of paramount importance in its impact on risk management decisions.

3. Risk Control: There are three basic methods for controlling risks: avoiding certain activities, reducing risks, and eliminating the impact of these risks.

4. Risk Monitoring: Establishing systems for monitoring and controlling loan risks, interest rates, exchange rates, liquidity, and settlement, which define limits, must also allocate appropriate means for controlling banking operations and legal risks.

Chapter 5: Internal Control Systems and Record-Keeping

Article 1: Internal Control Systems

The bank must establish appropriate internal systems for the proper implementation of legislation and regulatory regulations, including the policies and procedures required to combat money laundering and terrorist financing. These systems must be reviewed periodically to determine the extent of compliance with their implementation, identify weaknesses or deficiencies, and take the necessary measures to address them, taking into account the following:

1. Establish a clear policy for combating money laundering and terrorist financing, approved by the board of directors or the regional manager of foreign bank branches, for the purpose of proper implementation of legislation and regulatory regulations issued in this regard. This policy must be updated on an ongoing basis.
2. Establish detailed written procedures for combating money laundering and terrorist financing, which clearly define duties and responsibilities in accordance with the established policy.
3. Ensure that the internal systems, policies, and procedures are capable of detecting unusual transactions or transactions involving suspicious customers, and that these transactions are brought to the attention of the manager responsible for the Anti-Money Laundering and Counter-Terrorism Financing Department. 4
4. Establish an appropriate mechanism to verify compliance with the internal systems established to combat money laundering and terrorist financing.
5. Establish systems that ensure the internal audit function, in coordination with the director responsible for the Anti-Money Laundering and Counter-Terrorism Financing Department, reviews the systems in place to ensure their efficiency and effectiveness in combating money laundering and terrorist financing, and proposes the necessary measures to address any deficiencies or update or develop them.

Article 2: Retention of Records and Documents

Banks must retain customer data in accordance with Anti-Money Laundering and Terrorism Financing Law No. 39 of 2015 and the period specified therein.

1- Types of Records and Documents to be Retained

The bank must retain the following:

a. Records and documents of customers and beneficial owners, including account opening applications and copies of their identification documents, whether natural or legal persons, as well as copies of correspondence conducted with them.
b. Records and documents related to transactions conducted with customers, including sufficient data to identify the details of each transaction.
c. Reports of unusual transactions and any evidence supporting the review of these reports.
d. Records related to suspicious transactions, including copies of notifications of transactions sent to the Anti-Money Laundering Department and related data and documents.
e. Records and documents of reports that have been decided to be retained by the director responsible for the Anti-Money Laundering and Terrorism Financing Department.

f. Records related to training programs, including all program data obtained by bank employees in the field of combating money laundering and terrorist financing, the names of trainees, the departments/departments in which they work, the content and duration of the training program, and the entity that provided the training, whether domestically or abroad.

2- Requirements for Records Retention

The bank must observe the following requirements when retaining the records and documents stipulated in the previous clause:

a. All records, documents, and reports must be kept securely, and backup copies must be kept elsewhere.
b. The storage method must be characterized by ease and speed of retrieval of the retained records and documents, such that any data or information requested is provided in full and without delay.

3- Retention Period

Records and documents shall be retained for a minimum of five years. The starting date for the retention period varies depending on the type, as follows:

a. Customer and beneficial owner records and documents: Shall be retained for a minimum of five years from the date of account closure, or from the transaction end date for transactions conducted with non-account holders.
b. Records and documents related to transactions conducted with customers: Shall be retained for a minimum of five years from the date of account closure, or from the transaction end date for transactions conducted with non-account holders.
c. Other Records and Documents: The following shall be retained for a minimum of five years:
    - Extraordinary Transaction Reports, from the date of issuance of the report.
    - Records of suspected transactions sent to the Anti-Money Laundering Department, from the date of submission, or until a final decision or ruling is issued regarding the transaction, whichever is longer.
    - Records of suspicious transaction reports and their documents that have been decided to be retained by the manager responsible for the Anti-Money Laundering and Counter-Terrorism Financing Department, from the date of the decision to retain them.
    - Records of training programs, starting from the date of completion of the training program.

Chapter 5: Due Diligence

Article 1: Due Diligence Measures

1- Timing of Due Diligence Measures

All banks and financial institutions must conduct due diligence measures in the following cases:

a. Before and during the opening of an account or establishing a relationship with any customer.
b. Any incidental transaction whose value reaches or exceeds the amount specified by the Central Bank of Iraq and the Anti-Money Laundering and Terrorism Financing Office, whether conducted in a single transaction or in the form of multiple transactions that appear to be related to each other.
c. Conducting incidental transactions in the form of local or international wire or digital transfers, regardless of their value.
d. Doubts about the validity, accuracy, or adequacy of previously obtained customer identification data.
e. Suspicion of money laundering or terrorist financing, regardless of any exemptions or specific limits referred to in the law or any other regulations, instructions, or legislative statements.

2- Customer Acceptance Policy

Banks must establish clear policies and procedures for their customer acceptance requirements, taking into account all factors related to the customer, their activities, nationalities, associated transactions and accounts, and any other indicators related to customer risk. These policies must include a detailed description of each customer according to their risk levels and the basis upon which the business relationship with the customer will be classified. The following must also be taken into account for customers with high risks:

a. The bank must pay special attention when taking measures to identify these customers and their legal status.
b. The policies and procedures must include a description of the categories of these customers.
c. These policies and procedures must be recorded in writing and approved by the bank's board of directors.

3- Basic Requirements for Due Diligence Measures

a. The bank must not establish a business relationship with a customer unless the identity of the customer, their related parties, and the beneficial owner has been determined and verified. B.
b. The bank must not provide services or products, or continue dealing with individuals, without verifying their documents and keeping a copy thereof. It must also not enter into business relationships under unknown, fictitious, or fictitious names.
c. The bank must periodically evaluate the customer's normal business activities based on the expected pattern of their activities. Any unexpected activity must be examined to determine whether there is any suspicion that it may be related to money laundering and terrorist financing. In assessing unexpected activities, the bank must obtain and maintain information on:

    - The nature of the potential business.

- Pattern of transactions.
- Purpose of the transaction or account opening.
- Nature of the activity.
- Persons authorized to act on behalf of the customer or the signatories to the account.
- If the bank does not obtain satisfactory proof of identity before establishing a business relationship, it should consider submitting a report on suspicious transactions to the Anti-Money Laundering and Counter-Terrorism Financing Office.
- The bank must establish special systems to identify the identity and legal status of customers and beneficial owners, whether natural or legal persons, in the following cases:

    - When establishing an ongoing business relationship, whether upon opening an account or upon initiating any transaction.
    - When suspicions arise at any phase of dealing with the customer or beneficial owner. In all cases, this identification must include identifying the customer's and beneficial owner's activities.
    - When conducting any incidental transaction (including multiple transactions that appear to be related to each other) if their value exceeds $10,000 or its equivalent in Iraqi dinars and other currencies.
    - When conducting incidental transactions in the form of wire transfers exceeding $10,000 or its equivalent in Iraqi dinars and other currencies. The same procedure applies to the beneficiaries of the transfer, ensuring that complete data is collected in all cases.
    - When there is a suspicion or doubt about the occurrence of a money laundering or terrorist financing operation.
    - When there are doubts about the accuracy or sufficiency of previously obtained data to identify customers.

d. When determining the identity of the beneficial owner, banks must take the following steps:
    - The identity of the customer and the beneficial owner must be identified and verified, whether the customer is an individual or a legal entity, in accordance with the guidelines issued by the Anti-Money Laundering and Terrorist Financing Office.
    - The bank must determine for all customers whether the customer is acting on behalf of another person and must take all necessary steps to obtain sufficient identification data to verify the identity of that other person.

e. With regard to customers who are legal entities, the bank must take steps to:
    - Understand the customer's ownership and control structure.
    - Identify the individual or individuals who ultimately own or control the customer.
    - The bank must obtain information regarding the purpose and nature of the business relationship.
    - The bank must determine the extent to which due diligence measures are applied based on risk sensitivity.
    - The bank must be able to demonstrate to the banking supervision sector that the due diligence measures are appropriate and proportionate to the money laundering and terrorist financing risks. A bank must not accept the invocation of professional confidentiality from an agent, such as a lawyer, accountant, financial broker, or similar entity, when collecting identification information.

- A bank that belongs to a financial group must take into account the customer's activity with the group's various branches when implementing customer due diligence procedures.
- The bank should implement customer due diligence procedures on its existing customers based on the strength of the material evidence and the risks, and implement due diligence measures at appropriate times for existing business relationships. Examples of appropriate times to implement these measures include:
    - When a large financial transaction is being executed.
    - When a significant change occurs in the customer's documentation standards.
    - When a financial change occurs in the way the account is managed and operated.
    - When unusual transactions or transactions occur that deviate from the customer's normal trading pattern, based on the information available to the bank.
    - When an existing customer requests a new relationship or makes a fundamental change to the nature of the existing relationship.
    - When the bank realizes that it does not have sufficient information about an existing customer.
    - The customer's identity should also be verified by referring to the identification documents and signatures held by the bank. If these documents are incomplete, the customer shall be asked to provide them.

4- Reliance on a Third Party

a. When a bank decides to use another bank or financial institution to implement customer identification procedures, whether to complete the necessary data, verify the data provided, or rely on another intermediary, whether they are third parties or rely on them for this purpose, the ultimate responsibility for fulfilling the customer due diligence requirements rests with the bank concerned, not the third party.
b. The bank must only accept customers introduced to it by other financial institutions or intermediaries who have undergone due diligence measures that are equivalent to those approved by the Financial Action Task Force.
c. When a bank relies on third parties to perform certain customer due diligence procedures, it must obtain from the third party the necessary documents and information regarding aspects of the customer due diligence process and take appropriate steps to ensure that the identification data and other documents required within the framework of the customer due diligence process are consistent with the customer identification procedures.
d. The bank must ensure that the third party is subject to oversight and supervision and has appropriate procedures in place for customer identification and record-keeping requirements.
e. If the third party being used is located in another country, or if the bank has branches or subsidiaries in other countries, it must consider in which countries it can rely on a third party for customer identification, based on the information available to it regarding whether these countries adequately implement the FATF Recommendations.
f. Banks that rely on a third party for customer identification must obtain written confirmation from the third party that all due diligence measures required by the FATF Recommendations have been followed and that the identity has been identified and verified.
g. The bank must establish a direct communication channel with the customer after requesting documents, information, and recommendations from the third party.
h. The bank must provide details of the third parties it has relied on for the purposes of customer due diligence measures and notify the Banking Supervision Sector accordingly.

i. When the bank is not satisfied with the extent to which the identified party has complied with the requirements of the Financial Action Task Force (FATF) Recommendations, it must conduct its own customer due diligence measures regarding the business relationship for customer identification. It may also decline to accept any subsequent introductions from the identified party and consider discontinuing reliance on the identified party for the implementation of customer due diligence measures.

j. When the bank fails to complete customer due diligence measures satisfactorily, and the bank is unable to fulfill its obligations related to customer identification and customer due diligence procedures, it must take the following actions:
   - Not open an account for the customer or conduct any business relationship with the customer.
   - Notify the Anti-Money Laundering and Terrorist Financing Office, where appropriate.

j.

5- Completing Due Diligence Measures Following the Establishment of a Business Relationship

a. Customer identity verification may be completed for the purposes of customer due diligence measures to verify the identity of customers and beneficial owners following the establishment of a business relationship with the customer, provided that:
   - The risks of money laundering and terrorist financing are negligible and can be effectively controlled.
   - The verification procedures are completed as soon as possible, within a maximum period of one week.

b. If the customer or beneficial owner identity verification procedures are not completed within the aforementioned period, the bank must:
   - Not open the account, initiate a relationship with the customer, or carry out any transaction for the customer.
   - Notify the Anti-Money Laundering and Terrorist Financing Office immediately.
   - Monitor the risk management related to such customers.
   - Due diligence procedures to identify customers.

Article 2: Enhanced Due Diligence Measures for High-Risk Customers, Financial Transactions, and Financial Services

1. The bank must take enhanced due diligence measures and intensify ongoing monitoring when it becomes aware of a significant degree of money laundering or terrorist financing risk, and consider these additional measures in addition to the due diligence measures applied to all the aforementioned customers.
2. The bank must implement enhanced due diligence measures for high-risk categories, which are as follows:
   1. Non-resident customers, as they are considered high-risk customers due to their lack of a specific residence within the Republic of Iraq. Banks must ensure that the residency status of resident customers is renewed by the relevant authorities before carrying out banking transactions for them. The non-resident customer category includes customers, whether natural or legal persons, who do not have a permanent residence or address in the Republic of Iraq. The following must be taken into account when conducting procedures to identify these customers and their legal status: Enhanced due diligence must be applied to non-resident

customers. It is important not to open any bank accounts or deal in any way with non-resident customers unless they meet the following conditions:

- Know the purpose of the transaction.
- Know the validity of the residency status in the Republic of Iraq at the start of the transaction.
- Obtain a copy of the identity document and passport.
- Obtain the legal entity's articles of association certified by the competent authorities in the home country or the country's embassy in the Republic of Iraq.
- Obtain a copy of the business license or commercial registration document from the home country, signed and stamped by the competent authority in that country and certified by that country's embassy in the Republic of Iraq.

2. The designated non-financial businesses and professions include lawyers, notaries, dealers in precious metals, jewelers, real estate brokers, and accountants. Strict due diligence must be applied to the designated non-financial businesses and professions by the authorities responsible for licensing or authorizing the designated non-financial businesses and professions, or supervising them and ensuring their compliance with the requirements required by the Anti-Money Laundering and Terrorism Financing Law No. 39 of 2015. These include the Ministry of Trade, the Ministry of Industry, the Central Bank of Iraq, the Securities Commission, the Insurance Board, and any other body whose jurisdiction is decided upon as a supervisory body by a decision of the Council of Ministers based on the Council's proposal and published in the Official Gazette. The following are details of these professions and the bodies licensed and regulated by them:

    - Lawyers: The Iraqi Bar Association is responsible for licensing lawyers to practice their profession. Banks and financial institutions must verify the validity of their work licenses and membership in the association.
    - Real estate agents (brokers): The Ministry of Commerce/Chamber of Commerce is responsible for granting licenses to real estate agents.
    - Goldsmiths and precious metal dealers: The Ministry of Planning and the Central Organization for Standardization and Quality Control are responsible for granting licenses to goldsmiths and precious metal dealers. Banks and financial institutions must verify the validity of the work license issued by the Ministry of Planning, its validity, and its renewal by the specified dates, or provide a pledge to renew it within a period not exceeding three months from the effective date.
    - Accountants: The Iraqi Accountants Association is responsible for granting licenses to accountants after they have met all the requirements of the Accountants Association and the Professional Oversight Board.
    - The aforementioned non-designated financial businesses and professions are not equal in terms of relative importance and the degree of risk they are exposed to. However, they are all high-risk and require enhanced due diligence from banks and non-banking financial institutions.
    - Notary Public: Although the Financial Action Task Force considers the notary public profession to be among the non-designated financial professions, it cannot be counted among these professions in Iraq because it is a state-owned profession. Notaries public report to the Notary Public Department/Ministry of Justice, pursuant to Notary Public Law No. 33 of 1998. However, enhanced due diligence must be applied to notaries

public, as they hold the rank of general managers, pursuant to the aforementioned law, and all general managers are treated as persons exposed to risk by virtue of their positions.

3. Conducting enhanced due diligence for occasional customers with whom the financial institution does not expect to continue its business relationship. All licensed banks must consider the following:

    - Conducting due diligence measures for occasional customers.
    - Carrying out a transaction with a value of or exceeding $10,000 or its equivalent in Iraqi dinars or other foreign currencies, whether a single transaction or several seemingly related transactions.
    - There is any indication of suspicion of money laundering or terrorist financing, regardless of the transaction amount.
    - Doubts about the validity, accuracy, or adequacy of previously obtained customer identification data.
    - When providing any financial services to occasional customers in cases that do not require due diligence measures, the financial institution must request and retain basic information from the customer (customer name, nationality, ID number, transaction amount, currency, transaction date, and any other identifying information or documents in accordance with the requirements of this bank for each service provided by banks and non-banking financial institutions).

4. High-Risk Personnel: The following must be met: Enhanced due diligence applies to high-risk persons holding any of the following positions or functions, whether local or foreign, and their family members and those related to them:

    - The President of the Republic, his deputies, advisors, and those of similar rank.
    - The Prime Minister, his advisors, members of the Cabinet, and those of similar rank.
    - The heads of political parties.
    - The Speaker of the House of Representatives and its members.
    - The President of the Supreme Judicial Council and its members.
    - The heads of independent bodies and those of similar rank.
    - Undersecretaries, advisors, inspectors, and those of similar rank.
    - Ambassadors, ministers, plenipotentiaries, and diplomatic advisors.
    - General Managers And those of similar rank.
    - Court judges of various ranks.
    - Commanders and senior ranks in the security services and those of similar rank.
    - Heads of charitable institutions, non-governmental organizations, their agents, directors, and members of their boards of directors and those of similar rank.

5. The bank must take appropriate measures to exercise special due diligence on transactions conducted with persons from countries that do not implement the Financial Action Task Force (FATF) recommendations or do not implement them adequately, including legal persons and other financial institutions, and take stricter measures regarding them. Examples of such measures include:

- Carefully monitoring the transactions of these customers, identifying their purpose, and notifying the Anti-Money Laundering and Terrorist Financing Office if there is no clear economic purpose or if there are any doubts about them.
- Limiting business relationships or financial transactions with the aforementioned countries or persons from or present in those countries.

6. Business that is not conducted face-to-face and using modern technologies.
    - The bank must establish the necessary internal policies, procedures, and systems to avoid risks related to the misuse of technological developments in the field of money laundering or terrorist financing, and business relationships conducted through digital communication networks or by other means, such as mail services, online transactions, computer services, banking transactions via ATMs and other banking services, the use of automated teller machines (ATMs) by phone, the transmission of instructions or applications by fax or similar means, and the making of payments and receiving cash withdrawals as part of a digital transaction at a point of sale using prepaid cards, recharge cards, and stored-value cards linked to a bank account. Examples of these policies and measures include verifying the documents provided, requesting additional documents to complement the documents required from indirect customers, establishing independent communications with the customer, relying on third-party mediation, requiring the initial payment to be made through an account in the customer's name with another bank subject to the same due diligence standards, and other measures.
    - A bank must have specific and effective due diligence measures in place for customers with whom it does not deal face-to-face. These measures include ensuring that the customer is the real person and that the address obtained is the actual customer's address. These measures include, for example, calling the customer using previously obtained numbers, such as their mobile number, job title, or place of work. These measures also include contacting the employer or their supervisor at their place of work, with the customer's consent. They must also obtain detailed salary information through official channels and other available means, such as telephone or electricity bills, to verify the customer's address.
    - A bank that allows payments through digital network services must ensure that the monitoring of these transactions is the same as that followed for its other services, and that it has a risk-based methodology for assessing the money laundering and terrorist financing risks arising from such services.

7. Private Banking Services
    - A bank providing private banking services must establish appropriate policies and systems to identify and assess the risks arising from providing these services, taking into account the nature of these services, including:
        - Defining the purpose of implementing private banking services, including the volume and type of services to be provided to the customer, and the potential activity of the customer's account.
        - The development of the business relationship between the bank and the customer receiving the service.

- Private financial services are the activities through which a bank provides personal services to its high-net-worth clients. These services are typically performed through a central liaison officer between the client and the bank. This officer facilitates the client's use of the bank's private financial services and products, which include:

    - Dealing with various types of accounts.
    - Transferring funds.
    - Asset management and providing advisory services.
    - Lending (including credit cards and personal loans).
    - Opening letters of credit, issuing letters of guarantee, and collecting documents, including safekeeping of clients' securities.
    - Other various services for clients, whether banking, financial, or otherwise.

8. Due Diligence and Enhanced Due Diligence for Social Media Influencers: All licensed banks and non-banking financial institutions are required to exercise the utmost caution and vigilance regarding financial transactions made through the bank accounts, digital wallets, and digital payment cards of social media influencers. They are also required to develop scenarios for detecting money laundering transactions involving these individuals, tailored to these circumstances, in coordination with the Anti-Money Laundering and Terrorism Financing Office, if necessary. Enhanced due diligence measures must also be implemented regarding the financial transactions of digital store owners (owners of digital marketing websites and social media marketing).

9. Proxy Shareholders: Institutions are required to mitigate the risk of misuse of the proxy shareholders and proxy directors mechanism by exercising due diligence regarding them. This is achieved by implementing the measures taken by the Companies Registration Department regarding the provision of all information about the company, its shareholders, and its beneficial owners, according to a template prepared for this purpose. All branches of foreign companies are also required to provide the names and addresses of board members of foreign companies whose branches are registered, and update these information every six months.

10. In other cases:
    - Products with fictitious, digital, forged, or unnamed names.
    - Correspondence banking: When requesting to open facilities against deposits or when renting safe deposit boxes.
    - Correspondence payment accounts: When opening correspondent accounts, it is necessary to obtain a recommendation or signature authentication from a reputable bank.
    - Agency: When depositing cash or traveler's checks through a person or persons who do not represent the account holder by virtue of an agency or authorization, banks must ensure that both the agent and the principal are subject to due diligence measures before entering into or participating in any transaction involving an agency, and that both the principal and the principal are considered clients.
    - Bearer negotiable instruments: The bank must have adequate policies, procedures, systems, and regulations to conduct due diligence to combat money laundering and terrorist financing (AML/CFT) for the risks associated with the use of bearer negotiable instruments. This also applies to the bank itself. Before a bank enters into or participates

in a transaction involving the conversion of a bearer negotiable instrument into a registered form for the purpose of paying dividends or capital, the bank must apply enhanced due diligence measures to the instrument holder or beneficial owner, considering them both as its clients.

- With regard to virtual assets, it is worth noting that the Central Bank of Iraq has prohibited the use of digital cards and wallets for the purpose of speculation and trading in digital currencies in any form, in accordance with the instructions of the Central Bank.

11. Prohibition of Transactions
    1. Opening or maintaining numbered accounts, or any anonymous accounts or relationships, or fictitious or fictitious names.
    2. Dealing with anonymous persons or persons bearing fictitious or fictitious names.
    3. Dealing with shell banks.
    4. Dealing with any natural or legal person whose profession is to provide any of the activities, services, or operations designated for subject entities or virtual asset service providers in accordance with the legislation, without a license or registration, whether for the benefit of its customers or on their behalf.

Article 3- Simplified or Reduced Due Diligence Measures

1. The bank may apply simplified or reduced due diligence measures where there are circumstances in which the risk of money laundering or terrorist financing is low.
2. The bank may apply simplified due diligence measures to customers, transactions, or products that may present low risks, as follows:

    a. Government ministries, agencies, and institutions.
    b. Financial institutions subject to anti-money laundering and counter-terrorism financing requirements that comply with the requirements set forth in the law, the implementing regulations, these regulations, and the Financial Action Task Force (FATF) recommendations, and which are monitored for compliance with these requirements.
    c. An occasional or completed transaction in which the transaction size is less than one million Iraqi dinars or its equivalent in other currencies. The customer's name and contact information may be obtained.
    d. When conducting occasional transactions for a passing customer in the form of wire transfers with a value less than one million Iraqi dinars or its equivalent in other currencies, the customer's name and contact information may be obtained.
    e. A bank wishing to apply simplified due diligence to the aforementioned customers must retain supporting documentation to support the classification it assigns to the customer.
    f. Simplified due diligence measures may not be applied in cases where the bank knows, suspects, or has reason to suspect that the customer is involved in money laundering or terrorist financing activities, or that the transaction is being conducted on behalf of another person involved in money laundering or terrorist financing activities.
    g. Simplified due diligence measures may not be applied in cases where the bank knows, suspects, or has reason to suspect that the transactions are connected and that they aim to exceed the threshold amount mentioned in the two preceding paragraphs.

Article 4: Continuous Monitoring of Transactions

The bank must implement due diligence measures to identify customers when the transfer amount exceeds $10,000 or its equivalent in Iraqi dinars and other currencies, taking into account the following:

1. Outgoing Transfers
   a. The issuing bank must enter all required details and information related to the person requesting the transfer, whether the transfer is internal or external, and accompanying digital money transfers it conducts on behalf of its customers.
   b. The bank must implement due diligence measures to identify the person requesting the transfer, whether a natural person, a legal entity, or a non-profit organization. The bank must verify and maintain the accuracy of the information, and include it in full on the form through which the transfer is made. The minimum information required from the person making the transfer is as follows:
      - Name of the person requesting the transfer.
      - Account number or a unique or special identification number if there is no account.
      - Address of the person requesting the transfer.
      - Purpose of the transfer.
      - (Beneficiary information: name, address, account number, if available, etc.). For a customer making a transfer who does not have an account, the bank must complete their personal information and keep a true copy of their ID card/passport.

   c. The bank must verify all information in accordance with procedures before conducting any transfer. With regard to bulk transfers, the bank must include the account number of the person requesting the transfer, or their identification number if they do not have an account in their name, provided that the following is met:
      - The bank must retain all information related to the person requesting the transfer.
      - The bank must be able to provide the necessary information to the receiving bank within three business days from the date of receiving any such request.
      - The bank must be able to respond quickly and immediately to any order issued by the competent official authorities regarding a request to access this information.

   d. The bank must ensure that non-routine transfers are not sent within bulk transfers in cases that would increase the risks of money laundering and terrorist financing. These bulk transfer compliance requirements do not apply to transfers made by the bank for its own account, for example. In the case of spot foreign exchange transactions.

2. Inward Transfers
   a. The bank must adopt effective procedures and systems to identify and handle transfers that are not accompanied by complete information about the transfer applicant. This can be considered a factor when assessing the extent of suspicion regarding the transfer or related transactions, and then report this suspicion to the Information Collection Department.
   b. The bank must request the entity issuing the transfer to provide all incomplete information. If the entity issuing the transfer fails to do so, the bank must take appropriate measures based on the risk assessment, including rejecting the transfer.

c. If the beneficiary does not have an account, the bank must complete their personal information and retain a true copy of their identification documents (such as their national ID card, family card, or passport).
d. If the bank acts as an intermediary in the payment chain and performs the transfer, it must keep all information attached to the digital transfer form.
e. If the bank is unable to obtain the information accompanying the transfer for technical reasons, it must keep all other information available, whether complete or incomplete, for a period of five years.
f. If the intermediary bank receives incomplete information about the person requesting the transfer, it must inform the bank receiving the transfer of the transfer information. The bank receiving the transfer must refuse to accept the transfer if it does not include complete information about the person requesting the transfer.
g. These procedures do not apply in the following cases:
    - When the transaction is made using a debit or credit card, provided that the card number accompanies all transfers resulting from the transaction.
    - When the transfer is made from one bank to another, and if both the originator and beneficiary are banks acting on their own account.

3. The bank must pay special attention to internal reports on large, complex, and suspicious transactions and establish an integrated system that defines the mechanism for these reports, who is responsible for them, and how they are analyzed daily by the head of the Anti-Money Laundering Department.
4. The bank must establish an internal system that allows it to continuously monitor customer transactions to ensure they are consistent with the bank's available information about the customer and the nature of their activity. The degree of monitoring is determined by the degree of risk posed by the customer, the nature and size of their activity, their nationality, and their relationships with the outside world.
5. Conduct periodic or as needed reviews of current records, particularly those of high-risk customer categories, or when situations arise that require updating this data. Customer risk records are dynamically updated based on customer interactions through the customer risk management system, which is linked to the anti-money laundering and counter-terrorism financing system.
6. The bank must pay special attention to all complex or unusually large transactions and all unusual transaction patterns that have no apparent economic purpose or clear, legitimate purpose, such as large transactions relative to the business relationship with the customer, transactions that exceed certain limits, transactions in the customer's account that are inconsistent with the balance size, or transactions that deviate from the normal pattern of account activity. The background and purpose of such transactions must be examined, to the extent possible, and the findings must be recorded in writing and made available to regulatory authorities and external auditors for at least five years.

Article 5: Anti-Money Laundering and Counter-Terrorism Financing Regulations and Investigation and Investigation Regulations

First: Anti-Money Laundering and Counter-Terrorism Financing (AML) Regulations
All banks must operate in accordance with this regulation, which must include, at a minimum, the following:

1. Real-time monitoring of all transactions occurring in customer accounts, measuring and analyzing amounts withdrawn or deposited, along with specific customer cash flows in accordance with the Know Your Customer (KYC) principle, the account opening form (KYC), and the scenarios related

to money laundering and counter-terrorism financing approved by the Anti-Money Laundering Office, and issuing alerts on these scenarios on a timely basis.

2. The system classifies customer risks based on each customer's cash flows, the nature of their business, the geographical location of the business, the nature of the products, and the product delivery channels through which each customer deals. These risks are then identified and classified as high, medium, or low, at a minimum. Customer risk can be measured on a five-point scale.
3. This system should be directly linked to the comprehensive banking system (Core banking system) on the one hand, and to the platform for searching and investigating those included on local and international ban and sanctions lists on the other hand (Automatic Integration).
4. The aforementioned system uses artificial intelligence and machine learning algorithms to analyze data and identify potentially suspicious transactions. Accordingly, the Money Laundering and Terrorist Financing Reporting Officer (MLRO) sends suspicious transaction reports to the Anti-Money Laundering and Terrorist Financing Office (AML) via the GO AML system.
5. Analyze the patterns of financial transactions executed by the bank's customers and compare the volume of their transactions with the disclosed information.
6. Halt any transaction that matches one or more of the indicative suspicious scenarios until the bank's reporting officer verifies its validity, or halts transactions that the bank cannot tolerate after they have been identified by the Money Laundering and Terrorist Financing Reporting, Compliance, Risk, Audit, and Information Technology departments.
7. Identify customers exposed to risk by virtue of their position (PEPs) to ensure they are treated according to the associated risks and obtain the necessary approvals before commencing a business relationship with them.

Second - Search and Investigation Systems for Local and International Sanctions and Ban Lists

1. These are digital systems used to search for information related to individuals and entities subject to local or international sanctions, including the following:
   - The United Nations Security Council (UN) Sanctions List: This list lists the names of individuals and entities subject to international sanctions imposed by the UN Security Council.
   - The US Treasury Department's OFAC Sanctions List: This list lists the names of individuals and entities subject to international sanctions imposed by the US Treasury.
   - The European Union (EU) Sanctions List: This list lists the names of individuals and entities subject to international sanctions imposed by the European Union.
   - The Terrorist Assets Freezing Committee is a committee formed within the General Secretariat of the Council of Ministers that is responsible for freezing terrorist funds or other assets identified by the UN Security Council Committee.

2. Search and investigation procedures shall be conducted through the World-Check search and investigation system for all individuals and institutions wishing to deal with banks and other financial institutions. The search and investigation process must also include all parties involved, whether directly or indirectly, and identify the ultimate beneficiaries of the legal entities and arrangements with which the bank or financial institution deals.
3. It must be ensured that the approved search and investigation systems support the periodic updating of local and international sanctions and ban lists at least every 12 hours per day.
4. The search and investigation platform for those listed on the sanctions lists must support search capabilities in Arabic and English.

Chapter 6: Guiding Indicators for Identifying Transactions Suspected of Money Laundering or Terrorist Financing

Indicators for identifying transactions suspected of money laundering or terrorist financing depend on the bank's employees' familiarity with the provisions of the applicable Money Laundering and Terrorist Financing Law and the instructions issued pursuant thereto, as well as the experience gained from practical experience and specialized training in the field of combating money laundering and terrorist financing. The following are examples and scenarios of transactions that are the latest to be addressed by the Central Bank of Iraq and the Anti-Money Laundering and Terrorist Financing Office, as well as various banking transactions that require increased due diligence and scrutiny to identify the extent of suspicion of money laundering. New financial and banking instruments and technological factors affecting banking and financial activities are also taken into account. These scenarios represent the minimum that all financial institutions must follow to implement due diligence consistent with the financial operating environment in Iraq. Your institutions may develop new scenarios under the supervision and coordination of the Anti-Money Laundering and Terrorist Financing Office.

Article (1): Cash Transactions

Scenario Description

1. Unusually large cash deposits made by a natural or legal person (jurisprudent entity) that are disproportionate to the size of their business or employment activity.
2. Recurring cash deposits, whereby small amounts are deposited to avoid attracting the attention of bank employees, but the total amount over a specific period of time is disproportionate to the customer's business activity.
3. The customer's use of multiple accounts to deposit very large sums of cash within a short period of time.
4. Recurring cash deposits at multiple branches of the same bank within a short period of time, whether by the account holder himself or through other persons.
5. Large deposits and withdrawals made using ATMs to avoid direct contact with bank employees, especially if these deposits or withdrawals are inconsistent with the nature of the customer's business and normal income.
6. Large cash deposits and withdrawals from dormant or inactive accounts, or from accounts where the withdrawals are relatively large, or from accounts that have received unexpectedly large amounts from abroad.
7. Repeated withdrawals of funds shortly after depositing them without a clear justification.
8. The customer withdraws a portion of the amount to be deposited when the customer is aware of the need to follow due diligence procedures.
9. The customer provides financial statements about their business activity that clearly differ from those of similar companies operating in the same sector.
10. Frequent outward transfers or large amounts financed in cash, disproportionate to the size of the customer's business.
11. Companies with relatively large operations provide financial statements unaudited by a chartered accountant.
12. Depositing or withdrawing cash in multiple installments, such that the amount deposited each time is less than the limit set forth in the instructions issued by the bank, but the total amounts exceed that limit.

13. The customer suddenly repays a large debt without a clear explanation or reasonable source of repayment.
14. The customer exceeds their average withdrawal and deposit transactions.
15. The customer exceeds their average outward and inward transfers.
16. Cash withdrawal from the customer's account exceeding the limit declared in the Know Your Customer (KYC) form.
17. The customer's monthly income exceeds the expected income limit declared in the Know Your Customer (KYC) form.
18. The customer unexpectedly transfers the value of the facilities obtained outside Iraq.
19. Repeated transfers to the same beneficiary within a specific period of time.
20. Purchasing large amounts of bank checks in cash.
21. Receiving large amounts of checks endorsed by third parties for the customer's account.

Article 2: Transfers

1. Executing large-amount transfers abroad or receiving incoming transfers from abroad accompanied by cash payment instructions.
2. Recurring incoming transfers from different parties with no clear relationship to the customer, or those issued by the customer to these parties.
3. Transfers of equal or similar amounts to several people in different countries/or to a single beneficiary on multiple accounts.
4. Large-amount local transfers followed by transfers abroad in different currencies.
5. Directly transferring account deposits abroad, whether in one or multiple installments.
6. Receiving large transfers from abroad to inactive accounts.
7. Recurring outgoing transfers or large-amount transfers funded in cash, disproportionate to the customer's business.
8. Recurring transfers whose total over a specific period is disproportionate to the customer's business.
9. Using the customer's account as an intermediary account to transfer funds between parties or accounts.
10. Outgoing or incoming transfers with similar durations.
11. Outgoing or incoming remittances to countries and geographic locations classified as high-risk or included on local sanctions lists (asset freeze lists or international sanctions and embargo lists).
12. Incoming remittances that are then transferred within the same period or shortly thereafter.
13. Outgoing or incoming remittances from and to high-risk individuals.
14. Unjustified similarity of personal information for several individuals (address, telephone number, birth date, passport number, etc.).
15. Different documents submitted for each incoming or outgoing remittance, based on the databases available to you.
16. Refraining from presenting the sender's and recipient's passports, which are used to verify names on local and international lists.

Article 3: General Scenarios Related to Money Laundering and Terrorist Financing

Adopting the specific scenarios for combating money laundering and terrorist financing prepared by the Anti-Money Laundering and Counter-Terrorism Financing Office as a minimum for the digital systems you approve that are compatible with the financial operating environment in Iraq, in addition to the following:

Scenario Description

1. If an account has been inactive for a period of time (dormant account) and then becomes active without a reasonable cause.
2. Exchanging large quantities of small-denomination banknotes for large-denomination banknotes without a clear reason.
3. Unusually high cash deposits, then withdrawing them by means of checks and transferring them to other accounts repeatedly without a clear and convincing reason, especially if these deposits are transferred shortly after their deposit.
4. Not using credits in foreign trade transactions and keeping financial transfers in cash.
5. Lack of a reasonable justification for the customer choosing a bank branch to settle banking transactions.
6. The customer's refusal to provide the necessary information or documents required for the due diligence procedures.
7. The customer's refusal to obtain banking facilities, which are among the additional benefits the institution provides to its customers, to avoid providing any information that might lead the bank to discover the true nature of the activity.
8. A number of customers approach the bank to exchange the national currency for various foreign currencies without any indication of the customer's need for this.
9. Customers who frequently travel to countries known for drug trafficking, production, or illicit trade.
10. Customers who make fixed deposits without opening deposit accounts (as a casual customer).
11. Suspicious customer behavior, which manifests itself in clearly nervous behavior, sometimes accompanied by threats to the bank employee, in an attempt to dissuade the employee from fulfilling their duty of completing a suspicion report or verifying their identity.
12. Customers whose deposits contain counterfeit and heavily soiled banknotes that appear to have been used and stored extensively.
13. Clients who maintain multiple bank accounts not required for their work, especially if banking transactions involve the names of unknown persons.
14. Depositing large amounts of checks, where the beneficiary is a third party and the depositor is in favor of the client, with no clear relationship between the beneficiary and the client requiring this, or where the deposit is inconsistent with the client's profession or the nature of his or her business.
15. Multiple, recurring transfers from abroad to a single account, involving amounts less than the reportable limit of $10,000.
16. Remittances from or to countries known for their adherence to banking secrecy.
17. Individuals or companies that attract large sums of money to invest in foreign currencies or other negotiable instruments, where the volume of transactions is inconsistent with the interests of the individuals or companies involved.
18. Repeatedly buying or selling securities without a clear purpose.
19. The customer suddenly repays long-term loans without disclosing the sources of the funds, and obtains bank facilities or credit loans secured by jewelry or real estate mortgages, and repays them before their due date.
20. Customers requesting loans secured by assets owned by others with whom they have no clear relationship.
21. Different accounts are opened linked to the same beneficiary or agent, with the same data, addresses, and functional information provided for all accounts. The purpose of these accounts is to issue digital payment cards for use abroad.

22. Open source reports indicate that a person or entity's name or information has been linked to a previous crime or criminal record, particularly those related to human trafficking, migrant smuggling, or international sanctions.
23. Attempts to open accounts using documents that appear to be forged.
24. The customer's relatively young age, with the purpose of opening the account, the source of the funds, or the value of the transactions to be carried out on the account unclear.
25. A third party translates or gives instructions to the account holder when withdrawing or depositing funds into the bank account, especially during peak banking hours. A third party may always possess the customer's ID.
26. An unjustified lifestyle that is inconsistent with the business activity, as profits/deposits are significantly higher than those of counterparts working in similar professions/businesses.
27. Financial transactions by or with persons or entities about whom the bank has previously filed suspicious activity reports with the Anti-Money Laundering and Counter-Terrorism Financing Office.
28. Financial transactions by women, particularly those of younger age groups, are inconsistent with the nature of their business, or their frequent transfer or receipt of funds through the bank or bank agents (Western Union, MoneyGram) are inconsistent with this external activity.
29. Financial transactions by some legal entities, such as beauty salons and others, are inconsistent with the nature of their usual business, or foreigners are handling these accounts.
30. Negative information appears on open sources regarding a client's involvement in crimes of sexual exploitation, marriage of girls, or other suspicions.
31. Cash deposits to doctors, nurses, medical professionals, and hospital staff that are disproportionate to their work and experience.
32. Unjustified transactions between charities or their employees and entities and individuals unrelated to the field of humanitarian charitable work.
33. Transactions via multiple accounts and multiple authorized signatories on the account with no clear relationship between them.
34. The beneficial owner is from countries or regions known for criminal activity or high-risk countries.
35. The client changes the payment address stated on the documentary credit or invoice.
36. Suspicion of understating or inflating prices on invoices.
37. Multiple credit cards are issued to the same person within a short period of time.
38. The client held a high-ranking government position, and the entire balance of his account was withdrawn in dinars and deposited in dollars.
39. Withdrawals from the customer's account were made through an ATM located in a high-risk area far from the customer's residence address, which may indicate that the card is not in the customer's possession and that the customer is not the true beneficiary of the account.
40. Suspicion of illicit foreign exchange trading resulting from the customer's credit card being loaded with a cash deposit in local currency, followed by cash withdrawals in US dollars from ATMs outside the country.
41. Repeated use of the customer's credit cards for large purchases in US dollars outside the country.
42. Depositing a cash amount and linking it to a term deposit, inconsistent with the customer's young age and qualifications, and the nature of his activity being unclear.
43. Failure to ascertain the purpose of a transfer issued by a bank customer to a customer's account at another local bank, as well as failure to establish the relationship between the two.
44. Repeated deposits made to individual bank employees without specifying the relationship between them.

45. A client repeatedly receives small cash transfers from several people from different countries, which is inconsistent with her being a housewife with an unknown occupation, in addition to the lack of clarity in the relationship between her and the transferees.
46. Suspicion of the use of credit cards in virtual currency speculation and the transfer of funds from unknown parties in the form of a deposit to the card.
47. Purchasing a single-premium insurance policy for a large sum, and withdrawing a portion of it within a short period of time, inconsistent with the nature of the customer's business.
48. A customer working in social media receiving cash transfers from abroad into his account in amounts less than the prescribed limit, on a piecemeal and continuous basis.
49. A female customer depositing a large sum of cash with supporting evidence of a recent divorce certificate for a marriage contract, and then making piecemeal transfers to a person or group of people with whom she has no relationship.

Article 4: Documentary Credit Transactions

1. Importing or exporting goods whose type or value does not match the nature of the customer's business and activity.
2. Indications of a significant discrepancy between the value of the goods indicated in the documentary credit and their actual value.
3. The customer requesting, without clear justification, to amend the name of the beneficiary of the documentary credit before payment.
4. Opening multiple letters of credit inconsistent with the customer's business.
5. Opening letters of credit against financial guarantees inconsistent with the customer's business volume and history of dealings with the bank.
6. Having payment terms that appear unusual or paying to third parties with no clear connection to the letter of credit.
7. The beneficiary of the documentary credits must be companies owned by the customer, or the shipping companies must be owned by the customer.
8. The amounts stated in the documentary credit documents submitted by the customer to the bank do not match the original.
9. The customer changes the place of payment in the documentary credit to an account in a country other than the beneficiary's country.

Article 5: Letters of Guarantee

1. Multiple issuance of letters of guarantees inconsistent with the nature and scale of the customer's business.
2. Issuing letters of guarantee against financial guarantees that are not commensurate with the scale of the customer's business and the history of their dealings with the bank.
3. The beneficiary requests letters of guarantee without clear justification shortly after they are issued by the bank.
4. Issuing letters of guarantee at the customer's request without existing project contracts.

Article 6: Credit Facilities

1. Requesting a loan secured by assets owned by others, or borrowing customers providing additional guarantees owned by others, without a clear connection between them.
2. Obtaining credit facilities against collateral from a bank operating abroad without a clear reason.
3. The borrowing customer's request to quickly transfer the loan amount to other banks abroad without a clear purpose.
4. Unexpected early repayment of bad debts from the customer or other parties before the specified date.
5. The customer's purchase of certificates of deposit from time to time and their subsequent use as collateral to repay the facilities.
6. Obtaining credit facilities against the deposits of a company or subsidiaries abroad, particularly in countries known for drug cultivation or trafficking.
7. Obtaining credit facilities secured by cash deposits.
8. The customer's sudden repayment of a large debt without a clear explanation or reasonable source of repayment.
9. Circumstances surrounding the request for facilities that lead the bank to refuse to grant these facilities due to complaints about the validity and accuracy of the guarantees provided.
10. The customer submits unaudited financial statements.

Article 7: Digital Banking Services (Internet Banking, Telephone Banking, Internet Payment Services)

1. The account receives several small financial transfers digitally and then makes larger transfers abroad using the same method.
2. Depositing or receiving large payments regularly digitally from countries known for drug cultivation and production, or arms or human trafficking.
3. Existing online transfer transactions between the customer's accounts multiple times without any clear reason.
4. Depositing large payments regularly using various digital deposit methods, or receiving large payments regularly from other countries considered high-risk.
5. The customer requests to open an online account by submitting forged, misleading, or incorrect documents, enabling them to obtain services and facilities that are considered a preferential advantage for the customer.
6. Using digital banking channels to make repeated outgoing transfers to different people without a clear justification.
7. Sending and receiving remittances in high-risk countries by accessing online banking applications.
8. Using various technological means to make money transfers and changing access IP addresses to conceal traceability.
9. Transferring funds from several prepaid accounts to the accounts of other individuals or entities.
10. Obtaining various services in multiple locations in different geographic regions and in different currencies.

Article 8: Digital Payment Cards (Debit, Prepaid, and Credit):

1. Customers repeatedly use the full balance of the card, then pay the full debit balance.
2. Repeatedly withdrawing the maximum daily cash withdrawal limit for the card.
3. Always replenishing the account, not making any transactions or conducting a few transactions, and then withdrawing those funds.
4. Requesting transfers between the customer's accounts or with other authorized persons without justification.
5. Feeding the customer's account through cash deposits via ATMs in a specific currency, followed by withdrawals in another currency through the ATM.

Article 9: Foreign Exchange Transactions

1. Conducting repeated purchases or sales of foreign currencies, the total of which, over a specific period of time, is not proportional to the customer's activity.
2. Identifying a person from a third party located in countries known for drug cultivation and trafficking.
3. Conducting frequent and unexpected internal or external cash transfers in relatively large amounts in foreign currency.
4. The customer's refusal to provide sufficient and comprehensive information about the sources of the foreign currency he is depositing.
5. Attempting to conceal the identity of the true beneficiary of the transactions by conducting a series of consecutive foreign currency transactions.
6. The source of his funds and the level of income declared in the Know Your Customer (KYC) form do not match his foreign currency deposits.

Article 10: Safe Deposit Rental Services

1. The customer makes unusually frequent visits to his safe.
2. Non-resident customers in the exchange area keep safes without clear justification, especially if this service is available at banks operating in their area of residence.
3. Extensive use of safe deposit boxes, which may indicate the customer's ability to deposit large amounts of money in these boxes.
4. Customers who rent numerous safes without clear justification.

Article 11: Digital Securities Trading, Settlement, and Clearing Systems:

1. Transacting large sums of money without having a minimum level of knowledge of the nature of securities investment and its risks.
2. Depositing a cash amount to purchase securities for long-term investment purposes, and then selling the securities and withdrawing the funds shortly thereafter.
3. Always replenishing the account, not conducting any transactions or conducting a few transactions, and then withdrawing those funds.
4. Requesting transfers between the customer's accounts or with other persons authorized to transact on their behalf without justification.

5. Transacting large sums of money without a minimum level of knowledge of the nature of securities investment and its risks. 6. Depositing a cash amount to purchase securities for long-term investment purposes, and then selling the securities and withdrawing the funds shortly thereafter.

Article 12: Customer Behavior

1. Avoiding direct contact with bank employees, such as constantly using ATMs and evading bank officials whenever they attempt to contact them.
2. Signs of anxiety and confusion appear on the suspected customer or their representative during the transaction.
3. The customer or suspect has multiple bank accounts without a clear justification.
4. Urgently inquiring about bank records and instructions to obtain sufficient information about money laundering and terrorist financing operations to avoid legal violations related to them.
5. The customer requests excessive confidentiality regarding certain transactions.
6. The suspected customer or their representative requests the cancellation of a transaction as soon as bank employees attempt to obtain missing important information.
7. The customer shows dissatisfaction and unwillingness to complete a specific financial transaction when they learn that it requires reporting its details to the competent authorities.
8. A customer who behaves in an abnormal manner, such as failing to take advantage of opportunities to earn high interest on a large account balance and being ignorant of the basic facts related to the financial transaction.
9. A customer who refuses to provide the bank with the necessary identification documents.
10. A student customer who irregularly requests to issue or receive remittances or exchange currency for unusually large amounts that are inconsistent with their status.
11. A customer who is controlled by another person when they visit the bank and is unaware of what they are doing, or who is elderly and accompanied during the financial transaction by someone unrelated to them.
12. A customer who attempts to offer unjustified gifts or bribes to a bank employee, or attempts to persuade the employee not to verify identity documents.
13. A customer whose personal, home, or work phone is disconnected and unreasonably inactive.
14. A customer who refuses to disclose details of their work-related activities or disclose data, information, or documents related to their institution or company.
15. A customer who provides the bank with a permanent address located outside the bank's area of operation or one of its branches.

Article 13: Other Indicators

1. Transactions through multiple persons and the presence of multiple authorized signatories on a single account with no clear relationship between them, especially those of foreign nationality.
2. Use of bank accounts belonging to other persons.
3. The beneficial owner is from an area known for criminal activity.
4. Customers whose accounts are used to receive and spend large sums of money, with no clear purpose or clear relationship to the account holder and their business.
5. Accounts that receive multiple cash deposits or transfers and are then closed after a short period or left dormant.
6. Signs of excessive luxury and affluence on the suspected customer and their family, disproportionate to their financial status, especially if this occurs suddenly.

7. The suspected customer, the beneficial owner, or one of the parties to the transaction has a criminal record.
8. Purchase of high-value real estate, transportation, jewelry, or other property.
9. Evidence of forgery in documents, papers, or records.
10. The presence of parties to the transaction, including the suspected customer, the beneficial owner, or others, who are the subject of investigations by a third party.
11. The presence of fictitious contracts with other parties.

Article 14: Employee Behavior and the "Know Your Employee" Policy

First: The behavior of a bank employee is an indicator of their involvement in illegal transactions, as reflected in the following:

1. A significant and sudden increase in the employee's standard of living and spending, disproportionate to their monthly income.
2. The employee's reckless disregard for regulatory procedures and evasive behavior while performing their duties.
3. The employee's assistance in carrying out transactions where the beneficiary or counterparty is not fully known.
4. The employee's exaggeration of the customer's credibility, ethics, ability, and financial resources in reports submitted to the bank's management.
5. The employee's remaining after the end of official working hours without any justification.
6. Clear and noticeable neglect of their job duties, without any justification.
7. Possessing assets or property that are not entirely commensurate with their salary and monthly income.
8. Dealing with suspicious individuals and entities known for their lack of integrity.
9. Failure to maintain the institution's confidentiality, and disclosing or revealing confidential and important documents.

Second: Implementing the Know Your Employee (KYE) Principle
All banks and financial institutions must exercise due diligence toward their employees to prevent any suspicious or illegal activities. This can be done through the following:

1. All banks and financial institutions must implement the Know Your Employee (KYE) principle, ensuring the identification of any possible cases of internal collusion that may occur.
2. Organizing the Know Your Employee (KYE) form, with the Compliance Department monitoring banks' compliance and including its results in the semi-annual report sent to the Central Bank of Iraq.
3. Granting all bank employees a mandatory two-week continuous leave throughout the year, including managers and employees of the control departments, without any deductions.
4. Encourage your bank's managers and employees to attend specialized training courses in compliance, anti-money laundering, anti-corruption, and anti-fraud. This training should be conducted periodically to ensure continuous monitoring and keeping abreast of the latest methods and developments. This training should include all employees, not limited to managers, and no fees should be deducted from their salaries for these courses.
5. The necessity of rotating branch managers every five years at most, and not allowing them to manage the same branch for a period exceeding three to five years.

6. Credit authorities should not be granted to branch managers or employees except through credit products with specific purposes and conditions and within specific amounts.

Chapter 7: The Concept of Terrorist Financing

Terrorist financing: Any act committed by a person who, by any means, directly or indirectly, voluntarily provides, collects, or attempts to do so, from a legitimate or illegitimate source, with the intent to use them, knowing that these funds will be used, in whole or in part, to carry out a terrorist act or terrorist organization, whether the crime occurs or not, and regardless of the country in which the act occurs or the terrorist or terrorist organization is present.

Phases of Terrorist Financing

The terrorist financing process goes through three phases, regardless of whether the source of the funds is legitimate or illegitimate:

Phase 1: Fundraising

The process of raising funds to support and finance terrorist organizations depends on the size of the terrorist organization. Simple (small) or individual terrorist cells require relatively small amounts of money for use in terrorist operations. The smaller the terrorist cell or organization, the more difficult it is to detect and track it under the regulatory systems implemented by financial institutions and the anti-money laundering and counter-terrorism financing systems. Conversely, complex (large) terrorist cells require large sums of money and greater effort in raising funds to support all their members and cover operational expenses such as travel, airline tickets, training, subsistence, personal and medical expenses, promotion, and recruitment. Fundraising for terrorist organizations is carried out in one of the following ways:

A - Charities and Non-Profit Organizations

Charities and non-profit organizations are among the entities that are misused or abused by financiers and terrorists to raise and launder funds for terrorism. Because they enjoy public trust, have access to significant sources of funding, and are often located near conflict zones that may be vulnerable to terrorist activity, charities are typically established in conflict zones for humanitarian aid and assistance to affected people. Terrorists exploit charities and non-profit organizations by using them as a safe haven for money transfers in and around high-risk areas. Furthermore, funds collected for humanitarian aid in other countries may be mixed with funds collected to finance terrorism.

B - Funding from Legitimate Sources

Terrorist organizations sometimes rely on establishing legitimate investment projects as a cover for their operations, providing a sustainable source of income, separate from funds directly used to finance terrorist activities. This makes it more difficult for financial institutions to distinguish between financial transactions carried out routinely and daily and financial transactions actually used to finance terrorist activities.

C - Self-Directed Sources of Funding

These are the sources through which terrorist organizations rely on themselves to secure their needs for the funds, weapons, and equipment needed to commit terrorist operations and to recruit foreign terrorist fighters. The most important of these sources are:

- Salaries.
- Sale of personal property. Small, short-term loans that are difficult to detect.
- Family assistance is provided to members of terrorist organizations.
- Terrorist organizations support each other, as established terrorist organizations provide financial assistance, weapons, training, and safe haven to new terrorist organizations.
- Using small economic projects.

D. Proceeds from Predicate Crimes

Financial proceeds from predicate crimes (fraud, theft, drug trafficking, counterfeiting of currency and documents, human trafficking, kidnapping for ransom, illegal arms trafficking, child sexual exploitation, and other crimes) are an important and rapid source of financing for terrorist activities. Therefore, terrorists attempt to conceal the proceeds of these crimes using methods and techniques similar to money laundering.

E. Other sources of fundraising

- Bank robbery.
- Theft of national antiquities, smuggling them, and selling them on international markets.
- Smuggling machinery, equipment, and equipment abroad.
- Smuggling oil and its derivatives outside Iraq.
- Imposing taxes and fees.
- Forcefully imposing taxes on local residents.

Phase 2: Money Transfer

There are many targeted channels through which terrorists move their funds, the most important of which are:

a. Banks: Terrorist financing through the banking sector takes a hidden route. It is difficult to distinguish financial transactions related to terrorist financing due to the presence of normal financial transactions in accounts on a daily basis, especially since some terrorist operations require only small amounts. The banking sector can be used to transfer funds used to finance terrorism through the following methods:
    - Cash deposits.
    - Bank transfers.
    - Use of credit cards, ATM cards, and prepaid cards.
    - Use of banking and digital channels.

b. Exchange companies: are among the most important channels targeted by terrorists for transferring their funds from one country to another, and even within countries themselves, due to their many characteristics that terrorists exploit. The most important of these characteristics are:
    - Low cost of money transfers.
    - Multiple systems used for money transfers.
    - The ability to transfer funds to high-risk countries or to regions and territories that do not implement effective anti-money laundering and counter-terrorism financing systems, such

as those implemented by banks. This provides terrorists with an advantage in financing their activities, while preventing the transactions from being traced.

- The purpose of money transfers (family assistance) is often from countries known to the company due to the relationship between the parties. Terrorists seek to conceal the true purpose of money transfers, and the risk lies in the potential use of these funds to finance terrorist activities.

c. Digital Payment Systems: is modern technologies that can be used to transfer funds and finance terrorism, as they are accessible from all countries worldwide to transfer funds quickly and easily. Furthermore, the lack of direct customer interaction using digital payment systems provides a convenient cover for terrorists and terrorist organizations to conceal their true identities.

Digital payment systems that are not subject to effective regulatory systems are the most vulnerable to hacking by terrorists and others, especially those located in regions or countries that lack effective anti-money laundering and counter-terrorism financing systems.

The possibility of terrorist organizations using virtual currencies, particularly Bitcoins, has also recently emerged through digital black markets, facilitating suspicious financial transactions using such currencies.

d. Cross-border Money Transfers: are one of the most dangerous methods used by terrorists to finance terrorism internationally. Borders between countries are targeted conduits for terrorists to transfer funds to countries in conflict zones or to countries neighboring conflict zones, with the aim of providing all forms of support to terrorist organizations present in those areas, such as recruiting foreign terrorist fighters, providing training and armament, and financing terrorist operations. Cross-border money transfers take the following forms:

- Physical transportation by a natural person, in their luggage, or in accompanying vehicles.
- Shipping currency or bearer negotiable instruments in containerized shipments.
- Sending currency or bearer negotiable instruments by mail by a natural or legal person.
- Transferring funds through unofficial ports.

Phase 3 / Use of Funds

Funds collected from terrorists are used to finance their various activities, including:

- Purchasing weapons, equipment, and ammunition.
- Training terrorist fighters to carry out terrorist operations.
- Paying salaries and benefits to fighters and terrorists.
- Purchasing chemicals used in the manufacture of explosives, such as sodium nitrate, acetone, and others.
- Promotion and recruitment, either directly or through the use of social media and media outlets.
- Financing terrorists' livelihoods (food, housing, transportation, etc.)
- Purchasing airline tickets, credit cards, and prepaid cards.
- Searching for safe havens for protection.
- Financing projects that generate financial proceeds that fund terrorist groups.

Suspicion Indicators for Identifying Transactions That May Involve Terrorist Financing

1. Accounts that conduct donations or receive transfers from local or foreign non-profit organizations, associations, or other entities, particularly if these entities are located in countries known to support terrorism.
2. Transactions conducted on the accounts of a non-profit entity that are inconsistent in terms of style or size with the entity's purpose and activity.
3. The presence of large donations, particularly from foreign entities, to the accounts of a non-profit entity, especially if there is no clear relationship between them.
4. Transfers received from or sent to countries known to support terrorism.
5. Transfers received to beneficiaries belonging to countries associated with terrorist activities.
6. The account holder's name appears on lists of persons designated as terrorists.
7. A dormant account with a small balance that suddenly receives a deposit or a series of deposits and subsequent cash withdrawals until the entire balance is withdrawn.
8. Transactions conducted focus on customer accounts with amounts below regulatory limits.
9. Opening an account for a foreigner without a clear reason justifying his residence in the country.
10. Bank accounts are managed by individuals whose names are similar to those on the lists of designated terrorists.
11. Cash deposits into the account from multiple parties followed by the issuance of a remittance or remittances to areas experiencing security/political conflict or neighboring areas.
12. Cash deposits followed by access to the same account through online financial services from areas experiencing security/political conflict or neighboring areas.
13. Receiving remittances from countries and regions experiencing conflict and security and political instability.
14. Remittances received from or to countries associated with terrorist activities, or on the list of countries that do not implement the Financial Action Task Force's recommendations.
15. Sending remittances to persons or entities about whom negative information has been received in the media, indicating extremist political tendencies, or from areas of conflict and political and security instability.
16. Individual accounts that receive large transfers from an unknown source, the stated purpose of which is to finance living expenses.
17. Avoiding disclosure of the customer's actual information.
18. Multiple customers sharing the same information without justification.
19. Any person or entity listed on international or domestic sanctions and embargo lists.
20. Accounts that receive multiple cash deposits or transfers and are then closed shortly thereafter.
21. Deposits or transfers from persons with no clear relationship to the account holder.
22. Deposits or transfers from third parties to the account of a high-risk customer.
23. Small and frequent deposits and transfers without clear justification.
24. Using the customer's ATM and credit cards from other parties without clear justification.
25. Using various technological means to conduct financial transactions and changing access addresses (IP addresses) to conceal traceability.
26. Exchanging large sums of money consisting of small-denomination banknotes for the same amount and currency, but with larger-denomination banknotes.
27. Receiving or collecting donations or transfers from a foreign entity to the accounts of charitable organizations and non-profit companies without any clear connection between them.
28. Individuals or companies who support extremism and racism through their various social media posts.

29. Reports issued by law enforcement agencies indicating that a natural or legal customer is under investigation in a case related to national security.

In addition to the indicators mentioned above, the Anti-Money Laundering and Counter-Terrorism Financing Guidelines issued by the Anti-Money Laundering and Counter-Terrorism Financing Office may be used to obtain all indicators related to terrorist financing and various financial transactions.

Chapter 8: High-Risk Countries

High-risk countries are countries with significant strategic deficiencies in their systems to combat money laundering, terrorist financing, and proliferation financing, and with non-compliance with the Financial Action Task Force (FATF) recommendations. FATF calls on all member states to implement enhanced due diligence measures with these countries and urges them to do so.

Based on Recommendation No. 19 (High-Risk Countries) issued by the Financial Action Task Force (FATF) and Anti-Money Laundering and Terrorist Financing Law No. 39 of 2015, banks and financial institutions are required to take the following measures with regard to high-risk countries:

1. All financial institutions are required to implement enhanced due diligence measures on business relationships and transactions with natural and legal persons and financial institutions from countries identified by the FATF as high-risk.
2. Implement enhanced due diligence measures that are effective and proportionate to the risks.
3. To take effective and proportionate countermeasures when necessary or in the event of any new developments regarding high-risk countries identified by the Financial Action Task Force (FATF).

The FATF assesses countries in terms of the formulation and enforcement of acceptable laws in the field of combating money laundering and terrorist financing, and places them on one of four lists:

a. Green (No Problems): These are countries that adhere to the FATF standards and have successfully maintained a strong anti-money laundering and counter-terrorist financing (AML/CFT) system.
b. Grey (Cooperative but Problems): These are countries that have not submitted concrete measures to address their strategic deficiencies in combating money laundering and terrorist financing. These countries pledge to follow a specific action plan to address their deficiencies.
c. Red (Non-Cooperative): These are countries that pose a threat to the integrity of the global financial system. The Financial Action Task Force (FATF) calls for enhanced measures when dealing with them and imposes a set of requirements on them to be implemented as quickly as possible.
d. Black (Non-Cooperative and Subject to Countermeasures): These are countries that do not comply with the FATF recommendations and are not subject to its oversight. These countries are banned from dealing with them and are subject to financial and economic sanctions imposed by the United Nations Security Council, pursuant to resolutions issued by it. These sanctions restrict the activities, operations, and business relationships of natural and legal persons from these countries.

All banks and financial institutions must take into account concerns regarding deficiencies and non-compliance with any anti-money laundering and counter-terrorism financing (AML/CFT) regulations in the countries included in the aforementioned categories, regarding business relationships and all transactions with natural or legal persons, and take the necessary measures commensurate with the degree of risk, as follows:

- Paying special attention to business relationships and transactions originating from and returning to those countries.

- Requesting additional information about the customer and related transactions.
- Reviewing business relationships with correspondent banks in those high-risk countries.
- Verifying the nature and purpose of the business.
- Identifying the sources of the customer's funds and assets.
- Update customer data (foreigners) periodically through the Know Your Customer (KYC) form to identify any changes that may occur.
- Obtain senior management approval to continue the business relationship.
- Enhance transaction monitoring.

Chapter 9: Preventing Proliferation

The latest version of the Financial Action Task Force (FATF) Forty Recommendations criminalizes the proliferation of weapons alongside the crimes of money laundering and terrorist financing. This requires all banks and financial institutions to exercise increased due diligence regarding this phenomenon by updating their policies and procedures to include preventative measures. Banks are also required to include in their preventative measures the freezing of any transactions suspected of supporting or financing proliferation without delay. The indicators for these measures are as follows:

Suspected methods and indicators of proliferation financing

a. The use of shell companies, front companies, and companies with complex ownership, particularly those established in countries with weak or non-transparent company formation systems, to conceal identity, ownership, or the identity of the beneficial owner.
b. Disguising themselves through the work of individuals residing in other countries. Proliferation financiers structure transactions and corporate operations to appear as legitimate operations in a low-risk country, often a neighbor of the sanctioned country.
c. Exploiting transactions through foreign financial institutions. Financial institutions belonging to a targeted country subject to financial sanctions may have correspondent bank accounts or relationships with foreign financial institutions. Correspondent banks conduct transactions on behalf of those countries, enabling them to access the global financial system. Instead of repatriating funds or other assets belonging to the sanctioned countries, those funds or other assets remain in bank accounts abroad, particularly in countries with no clear connection to the sanctioned countries, to facilitate their international trade through those accounts.
d. Exploiting the commercial relations of neighboring countries and the shipping networks of other countries. Some sanctioned countries have extensive commercial networks with surrounding countries and can access the global financial system through these networks. Sanctioned countries can also indirectly enter the global financial system through a group of countries with which they have commercial relations.

Guiding indicators for identifying transactions suspected of involving proliferation financing

a. Customer-related indicators
    - The customer requesting the transaction or the customer receiving it are similar to those of an individual or entity listed on the embargo and sanctions lists or known to be associated with financing activities.
    - The customer is involved in providing, delivering, or selling dual-use goods, strategic goods, or special military goods for high-risk countries.
    - The customer or recipient's address is similar to that of a designated individual or entity or has a history of export control violations.
    - The customer is involved in involving a person associated with a country of proliferation concern (e.g., a dual national or dealing with complex equipment for which they lack technical expertise).
    - The customer is a military or research entity affiliated with a jurisdiction with a high proliferation risk.

b. Indicators related to the customer's activities

- Involving an individual or entity in any country with a proliferation risk.
- The transaction reflects a link between representatives of companies exchanging goods to evade scrutiny. The two companies may share a common director and owner, or may share declared addresses, or the representative's residential address may be the same as the company's (administrative address).
- The shipment route is unjustifiably complex, and the related payment transactions are unjustifiably complex or indirect.
- The presence of an unexplained pattern of wire transfers related to dual-use goods, proliferation-sensitive goods, or military goods, whether licensed or unlicensed.
- The transaction may involve a sudden change in fund transfers.
- The financial transaction may be complex, unusual, or involve an unusual use of financial products.
- The presence of instructions or financial transactions on the account for the payment of funds or transfers to parties named in the underlying letter of guarantee or other transaction-related documents.
- It may include the shipment of goods inconsistent with normal geographic trade patterns, i.e., when the country in question does not normally export or import certain types of goods, or if the vessel is listed on international embargo and sanctions lists.
- It may involve the shipment of goods from companies or individuals from a country other than the declared ultimate beneficiary's country.
- Sudden and frequent changes in board members and authorized signatories that are not well explained or intended to conceal ties to individuals associated with sanctioned countries/activities.
- Inconsistencies in information contained in commercial documents and financial flows, such as names, companies, addresses, endpoints, etc.

c. Geographical Indicators

- The transactions involve individuals or entities located within a country known to be associated with proliferation financing activities.
- The transactions involve individuals, companies, financial institutions, or unspecified financial businesses and professions known to have deficiencies in combating money laundering and terrorist financing, deficiencies in export and import regulations, or deficiencies in implementing laws and regulations.
- The country receiving the transactions is a producer of dual-use goods or military goods.
- The transactions involve individuals or entities in foreign countries known to redirect funds to countries that assist in financing proliferation.

d. Suspicion Indicators Related to Commercial Documents

- The value of the shipment according to the accompanying documents is less than the cost of the shipment, or this discrepancy is noticeable.
- There is a discrepancy between the financial information available in the accompanying commercial documents and the financial flows, such as names, companies, addresses, and entity.

- This may include discrepancies between the goods described in the documents and the actual goods, or between the description of the goods shown in the shipping documents and the description of the goods shown on the invoices. May involve unwarranted third parties.
- The recipient of the transaction is another shipping company.

e. Suspicion indicators related to shipping and trade finance:
   - Evidence that documents or other statements (e.g., related to personal, customs, or payment) are false or fraudulent.
   - A shipping company is listed as the final front end for the product.
   - The goods are ordered from companies or individuals from countries other than the declared end-user's country.
   - The declared value of the shipment was clearly understated compared to the cost of shipping.
   - The transaction represents the shipment of non-compliant goods and the technical level of the country to which they are being shipped. For example, semiconductor manufacturing equipment is being shipped to a country with no digital industries.
   - A circuitous or circuitous shipping route for financial transactions.
   - The shipment of non-compliant goods and typical geographic trade patterns. For example, does the country in question typically export or import the particular commodity?
   - Include a shipping route (if available) through a country with weak export control laws or poor enforcement of export control laws.
   - The description of the goods in trade or financial documents is not specific or misleading.

Chapter 10: Correspondent Accounts (Correspondent Banking Relationships)

Given the significant importance of correspondent banks to the banking sector, through their ability to fulfill their obligations and those of their customers (i.e., in executing documentary credits, foreign transfers, etc.) and facilitating the country's trade with the outside world, and the significant risks associated with money laundering and terrorist financing operations, these two crimes are among the greatest challenges facing correspondent banks worldwide. Statistics indicate that many terrorist efforts have been financed, directly or indirectly, through money laundering operations within correspondent banks. Therefore, it is necessary to identify the risks of money laundering and terrorist financing and take the necessary measures to mitigate these risks.

In order to identify these risks, banks must conduct a comprehensive assessment of money laundering and terrorist financing risks, analyze the factors used in money laundering and terrorist financing operations, and identify suspicious persons or entities and deal with them appropriately. Therefore, all financial institutions must follow the following measures, as a minimum, when establishing a relationship with correspondent banks:

First: Determine the adequacy of policies, procedures, and internal regulations in dealing with correspondent banks and ensure that they comply with legal requirements.

1. Determine the extent of the institution's employees' compliance with internal policies, procedures, and regulations.
2. Determine the adequacy of the scope of internal and external audits in reviewing anti-money laundering and counter-terrorism financing activities in correspondent banking relationships.
3. Banks and financial institutions must ensure that policies and procedures are in place to identify the ultimate beneficiary of the real account holder, and that these policies support enhanced due diligence procedures for customers with direct access to the account.
4. Banks must conduct a comprehensive risk assessment related to correspondent banking, analyze the factors used in money laundering and terrorist financing operations, and identify suspicious persons and entities by periodically updating applicable policies and procedures.
5. Determine the adequacy of the correspondent account approval process.
6. Determine the adequacy of monitoring operations on correspondent accounts.
7. Identify and report on unusual transactions, both in terms of the volume and nature of the transactions being verified.
8. When conducting any transaction with correspondent banks, the beneficial owner who holds accounts with these banks must be investigated through official correspondence and documented exclusively through the SWIFT system.
9. Ensure that the following due diligence measures are taken when establishing a correspondent banking relationship with correspondent institutions:
    a. Collect sufficient information about the respondent institution to fully understand the nature of its business, determine its reputation, and the level of oversight it is subject to.
    b. Evaluate the correspondent institution's anti-money laundering and counter-terrorism financing regulations and ensure their effectiveness and adequacy.
    c. Obtain the approval of the institution's senior management before entering into a business relationship with correspondents.
    d. Clearly understand and document the responsibilities of each institution regarding anti-money laundering and counter-terrorism financing.

e. If the correspondent institution provides correspondent account services to its customers, the correspondent institution must satisfy itself that it has implemented due diligence procedures for its customers who have direct access to these accounts and that it has the capacity to provide information related to these customers when necessary.
f. Not to enter into or continue a business relationship with shell banks and not to deal with a financial institution that allows the use of its accounts from a shell bank.
g. Completing a written survey that clarifies the correspondent bank's compliance with its local legislation and regulatory regulations, the due diligence standards it applies to its customers, and the extent to which the correspondent bank has effective internal policies and procedures in this regard.
h. Ensuring that the correspondent banking relationship with any correspondent bank that does not comply with anti-money laundering and counter-terrorism financing requirements is terminated.
i. Identifying money laundering risks through the nature of the products offered by the correspondent bank, as follows:
    - Opening correspondent accounts.
    - Establishing overlapping relationships.
    - Establishing bearer payable accounts.

j. Identifying the characteristics and details of the correspondent bank, including:
    - The basic commercial products and services offered by the correspondent bank.
    - The correspondent bank's management, ownership structure, board members, and executive directors.
    - The correspondent bank's regulations, policies, and procedures related to combating money laundering and counter-terrorism financing.
    - Identifying international and local sanctions imposed on the correspondent bank, if any, and the bank's corrective actions regarding the imposed sanctions.
    - Knowledge of the environment and geographical location in which the correspondent bank operates, and ensuring the effectiveness of the laws, regulations, and supervisory oversight bodies within the same geographical location, according to the classifications issued by international institutions.

Second: In order for banks operating within the Iraqi banking system to be able to establish relationships with reputable correspondent banks at the global and regional levels, and to fully comply with international standards and requirements, banks must meet the following requirements:

1. The bank's final financial statements for the last three years must be audited by an external auditor from one of the ten largest firms in this field globally.
2. A report evaluating money laundering, terrorist financing, and compliance policies and procedures from one of the international institutions concerned with this field.
3. The bank's credit rating is from one of the international rating agencies recognized by the Central Bank of Iraq:
    - S&P
    - Fitch
    - Moody's
    - Capital Intelligence
    - Islamic International Rating Agency

4. Periodic and continuous updating of the bank's profile on the BANKERS ALMANAC website, which assists banks in establishing relationships with correspondent banks and in compliance with remittances, particularly those related to trade finance operations.
5. Involving the largest possible number of bank staff, particularly those involved in financial transfers, the Compliance Department, and the Anti-Money Laundering and Terrorist Financing Reporting Department, in specialized training courses in their field, and ensuring that the largest number of them obtain professional certifications in this field.

Chapter 11: Liaison Officers

To facilitate and enhance the procedures of all financial institutions regarding combating money laundering and terrorist financing, all banks must appoint a liaison officer in all bank branches and issue administrative orders to that effect. A replacement officer must be designated in the same administrative order in the event of their absence. A specific job replacement policy must also be adopted, including the appointment of competent replacements to replace the original employees and perform the same duties. The policy is summarized as follows:

1. The liaison officer is considered the assistant to the director of the Money Laundering and Terrorist Financing Reporting Department at the bank's branches.
2. A digital window for the AML/CFT system is opened for the liaison officer at the branch where they work. This window allows them to review all transactions within that branch and ensure that all relevant documents are attached.
3. The liaison officer signs the account opening form (KYC) on behalf of the director of the Money Laundering and Terrorist Financing Reporting Department and the assistant to the branches. The head office branch must be either the director of the Money Laundering and Terrorist Financing Reporting Department or their assistant, as the head office branch is often part of the general management of the bank.
4. Verify the supporting documents and papers submitted by the customer by comparing them with the person submitting them.
5. Ensure that the customer is not included on local and international lists after reviewing them. The customer is then provided with the lists of the terrorist funds freezing committee, which are published on the official website of the Anti-Money Laundering and Terrorist Financing Office or obtained through the department manager.
6. Submit suspicious activity reports exclusively to the Director of the Money Laundering and Terrorist Financing Reporting Department. The branch management has no involvement in this matter.
7. The liaison officer is fully dedicated to his work and is not assigned any other duties related to compliance and combating money laundering and terrorist financing.
8. The technical liaison officer's liaison with the Director of the Money Laundering and Terrorist Financing Reporting Department in the bank's general management is the sole responsibility. Administrative liaison with the branch management is the responsibility of the liaison officer.
9. The liaison officer is assigned a telephone number and email address to ensure confidential communication with the Director of the Money Laundering and Terrorist Financing Reporting Department in the general management.
10. He submits his monthly reports to the Director of the Money Laundering and Terrorist Financing Reporting Department at the Bank's General Management, no later than 10 days after the following month. His report includes the cases reported and the latest actions observed during the month, and is available upon request from inspection bodies.
11. The Bank shall involve him in training courses held for the Money Laundering and Terrorist Financing Reporting Department at the Bank's General Management, or any other training courses organized by the Bank.

Chapter 12: Cash Import

Based on Recommendation No. 32 of the Financial Action Task Force (FATF) Recommendations for Cash Transmitters, and in order to facilitate and enhance procedures for importing foreign currency from abroad for all banks wishing to do so, and taking into account the bank's due diligence measures for all parties involved in the import of foreign currency, as well as the Cash Import Instructions No. 4 of 2011, we list below the approved mechanism in this regard:

1. Authorized banks may import foreign currency from abroad, provided they obtain prior approval from their respective banks and provide the following details (the entity from which the currency will be imported, the entity responsible for importing the currency, the expected contract date, the contract duration, the number of imports, the value of the imported amounts each time, and the total amount to be imported).
2. The financial institution from which the foreign currency is purchased outside Iraq must be licensed, subject to the oversight of the monetary authority in its country, and committed to implementing anti-money laundering and counter-terrorism financing procedures.
3. The approval of the Central Bank of Iraq is conditional upon the bank requesting the import being in a sound financial position.
4. Imported foreign currency may be brought in exclusively by air and through airports affiliated with the Civil Aviation Authority.
5. The use of imported foreign currency shall be for the purpose of meeting customer requests from duly registered companies, organizations, and entities, as well as individuals working for foreign companies or institutions who receive inward remittances from abroad, taking into account all due diligence procedures in accordance with Anti-Money Laundering and Terrorism Financing Law No. 39 of 2015.
6. Provide this bank with the name of the foreign shipping company, along with a copy of the license granted to it in its country. This company must be a globally recognized company in the field of cash transportation, such as DHL Forwarding, GardaWorld, or Brink's Global, This must take into account due diligence procedures, research, and investigation of local and international sanctions and ban lists for all parties involved in the import of cash, whether these parties are the correspondent bank, the cash carrier, or the ultimate beneficiary.
7. The importing bank must provide the Central Bank of Iraq with detailed statements of the imported foreign currency, supported by the following:
    a. The amount of foreign currency imported and sold during the import shipment period, supported by import documents.
    b. Evidence supporting the purchase price of the imported foreign currency from outside Iraq and its selling price within Iraq, as this price will be verified against the price approved by this bank.
    c. Banks are required to record the serial numbers of these shipments and provide the Central Bank of Iraq with all data pertaining to their recipients.
    d. A copy of the license granted to the shipping company by its country

8. The bank importing the foreign currency shall:
    a. Provide comprehensive insurance for cash shipments to cover potential risks.
    b. Prepare the requirements for the arrival of the imported foreign currency shipments to Iraq.
    c. The bank shall bear the value of any invalid imported banknotes included in the shipments and inform the Central Bank of Iraq of them.

9. The Central Bank of Iraq may prohibit any bank from importing foreign currency for a period it deems appropriate due to the economic conditions related to the supply and demand for foreign currency within Iraq.

Chapter 13: Banking Secrecy

Banking secrecy laws require all financial institutions to ensure that the policies and procedures in place within the institution do not impede the implementation of any regulatory measures related to combating money laundering and terrorist financing. Furthermore, the financial institution's senior management must ensure that all policies, procedures, and regulations maintain and adhere to banking secrecy in accordance with Article 49 of Banking Law No. 94 of 2004.

Chapter 14: Deterrent Penalties

To ensure optimal implementation of the regulatory requirements for combating money laundering and terrorist financing, and to prevent those involved in money laundering and terrorist financing crimes from using financial and banking products and services as conduits for their illegal activities, the penalties and sanctions related to combating money laundering and terrorist financing, as stipulated in Banking Law No. 94 of 2004, Anti-Money Laundering and Terrorism Financing Law No. 39 of 2015, the Companies Law No. 21 of 1997 (as amended), and all penalties stipulated in applicable and relevant laws and instructions, are applied to violators of the aforementioned regulations from the date of their entry into force.

Chapter 15: General Guidelines

1. The bank must use all possible means to monitor suspicious transactions and operations, with a focus on transactions conducted through countries included in the list of non-cooperative countries and the lists of internationally pursued individuals and entities.
2. The bank must keep abreast of global developments in money laundering and terrorist financing patterns and measures to combat them, particularly those issued in this area by the Financial Action Task Force (FATF), the International Monetary Fund, the World Bank, the Basel Committee, and other international organizations.
3. The bank must know the source of funds deposited upon opening an account, particularly large cash deposits.
4. When managing dormant accounts, the bank must adhere to the following:
    a. Comply with the provisions of Article 37 of the Iraqi Banking Law No. 94 of 2004.
    b. Determine a specific time period for dormant accounts. After that period, these accounts must be transferred to the Central Bank of Iraq in accordance with the Dormant Accounts and Abandoned Funds Instructions No. 1 of 2009.
    c. Freeze dormant accounts not used by the customer for a period of six months, and only reactivate these accounts after meeting the following conditions:
        - The account owner or their legal representative must be present in person and present identifying documents.
        - Submit a signed application to reactivate the inactive account.
        - The account will be reactivated after review and signature by the branch manager and liaison officer based on the data provided.
        - The bank's Internal Control Department reviews account reactivation procedures at branches on a monthly basis.
        - In the event of tampering with customer accounts or failure to comply with the above, the bank bears all legal consequences.
        - The above instructions apply only to current accounts (individuals and companies) and do not include savings accounts, fixed deposits, government accounts, and bank accounts operated by digital cards.
            - No transactions may be carried out on these accounts except through the branch manager or their assistant.
            - Audit the monitoring of checks drawn on them.
            - No withdrawals from these accounts may be made except by check.
5. Programming the bank's automated system to prepare reports that help increase the efficiency and effectiveness of the bank's internal systems in combating money laundering and terrorist financing. The proposed reports include the following:
    a. Current account movement and balance reports, which include all accounts, whether for customers or employees, and include all transactions for each account over a specific period (monthly), the account balances at the end of each month, the average balance, and the number of transactions executed, enabling the identification of any unusual activity.
    b. Transfer reports: Include all incoming and outgoing domestic and international transfers, the amount of each transfer, the currency, and the payment method (cash or check) for each individual customer.
    c. Foreign bank account movement and balance reports: Include all transfers executed by any means, specifying the amount and currency, the name of the bank and the name of the beneficiary, as well as the number and size of transactions with each foreign bank, and any other changes.