Cham Bank

Cover Page
Internal

Particulars	**Details**
Document Name	Anti-Money Laundering and Counter-Terrorist Financing Guide
Document Number	P-COM-18
Document Owner	Cham Bank
Number of Pages	35
Document Version Number	04
Date of Issue	18/08/2024
Prepared by	Compliance Department

Version Type: Original Version

Preparation and Review

	Position	Name	Signature	Date
Prepared by	Department/Section Manager	Mr. Mohamed Afra Hatra	Signed	~~18/8/2024~~
Reviewed by	Quality Management Manager	Mrs. Rana Al-Ahmad	Signed	18/8/2024

Study and Review of Policies and Procedures by the Committee

	Member	Member	Member	Member	Committee Chairman
Name	Mohamed Afra Khadra	Ezzat Diab	Mohamed Bash	Mohamed Anas Sukkar	Abdulrazak Al-Qatrawi
Signature	Signed	Signed	Signed	Signed	Signed
Date	29/8/2024	29/8/2024	29/8/2024	29/8/2024	29/8/2024

|	**Approval by the Sharia Supervisory Board**	**Adoption and Circulation by the Chief Executive Officer**
Name	Amin Amin	Ahmad Al-Lahham
Signature	Signed	Signed
Date	29/8/2024	27/9/2024

Amendment table

	Location of Amendment	Date of Amendment	Responsible for Amendment	Approval of Amendment
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

Table of Contents

Introduction:

This guide is considered a unified operational charter containing all the approved policies and procedures at Cham Bank as a program for combating money laundering and terrorist financing. It aims to provide all bank employees at all administrative levels, including the Board of Directors, with the fundamental and expanded principles that must be adhered to in order to ensure the bank's compliance with the laws and decisions related to combating money laundering and terrorist financing, as well as appropriately responding to international requirements in this field, taking into consideration the recommendations issued by the Financial Action Task Force (FATF). Consequently, this protects Cham Bank from the risks that may result from the potential misuse of its accounts in money laundering or terrorist financing operations.

This guide has been developed based on the requirements of Legislative Decree No. /33/ of 2005 and its amendments by Legislative Decree No. /27/ of 2011 and Legislative Decree No. /46/ of 2013 concerning combating money laundering and terrorist financing, and the System for Monitoring Banking and Financial Operations issued by Decision No. /19/ of 2019 by the Management Committee of the Anti-Money Laundering and Counter-Terrorist Financing Authority and its amendments.

This guide must be reviewed and updated whenever necessary or when there is a material change in the bank's risks regarding money laundering and terrorist financing operations, or substantial amendments to the decisions and laws regulating anti-money laundering and counter-terrorist financing procedures. This guide is approved by the bank's Board of Directors or the bank's management as per authority. A copy is placed on the bank's electronic website and circulated to all bank employees for application as required.

I- Laws and Definitions:

1. Laws and Legislation Related to Combating Money Laundering and Terrorist Financing:

1-1 Legislative Decree No. /33/ dated 01/05/2005 on combating money laundering and terrorist financing and its amendments by Legislative Decree No. /27/ of 2011 and Legislative Decree No. /46/ of 2013.

1-2 The System for Monitoring Banking and Financial Operations, Decision No. /19/ of 2019 issued by the Management Committee of the Anti-Money Laundering and Counter-Terrorist Financing Authority on 13/03/2019, effective as of 01/04/2019, and its amendments.

1-3 Legislative Decree No. /30/ of 2010 concerning banking secrecy.

1-4 The Anti-Money Laundering and Counter-Terrorist Financing Guide adopted by Cham Bank, which defines the responsibilities of various parties within the bank within the general framework of the anti-money laundering and counter-terrorist financing program.

1-5 The bank's internal policies, procedures, and controls related to anti-money laundering and counter-terrorist financing procedures.

2. Approved Compliance Monitoring Management policies and procedures, including the procedures of the verification unit concerned with verifying the bank's compliance with anti-money laundering and counter-terrorist financing procedures.

3. Definitions

3-1. Definition of Money Laundering:

Legislative Decree No. (33) of 2005 defined money laundering as any conduct intended to conceal or disguise the identity of funds related to illicit operations, thereby camouflaging their true sources, to make them appear as if they resulted from legitimate operations.

The following acts are considered money laundering crimes:

a. Concealing or disguising the true nature of funds, their source, location, disposition, movement, ownership, or related rights, knowing that they are illicit funds.
b. Transferring or converting funds, knowing that they are illicit, for the purpose of concealing or disguising their source or assisting a person involved in committing the crime to evade liability.
c. Acquiring, possessing, managing, investing, or using illicit funds to purchase movable or immovable property or to conduct financial operations, knowing that they are illicit funds.

3-2 Definition of Terrorist Financing:

According to the instructions of Legislative Decree No. (33) of 2005, the commission of the crime of terrorist financing includes any act intended to provide or collect funds by any means, directly or indirectly, from legitimate or illegitimate sources, with the intent to use them wholly or partly in a terrorist act or to finance a terrorist organization or a terrorist person inside or outside the territories of the Syrian Arab Republic.

3-3 Anti-Money Laundering and Counter-Terrorist Financing Authority:

An independent body with judicial status, headed by the Governor of the Central Bank of Syria, responsible for all matters related to money laundering and terrorist financing. It has prosecutorial authority, and the competent courts have the power to adjudicate the matter.

3-4. Audit Committee:

A committee derived from the Board of Directors, responsible for monitoring the work of the Compliance Monitoring Department, including the verification unit, and the bank's compliance with the anti-money laundering and counter-terrorist financing program.

3-5: (FATF)

The Financial Action Task Force is an intergovernmental organization established in 1989 on the initiative of the G7 nations, which issued the 40 Recommendations on measures to combat money laundering and terrorist financing. It assesses countries' compliance with these recommendations.

3-6 Offshore companies

Companies established in one country but operating in another. They are considered high-risk accounts.

3-7 PEPs

Politically Exposed Persons. A foreign person holding a prominent political, security, or military position is considered a PEP. A Syrian person assigned a significant mission by an international organization is also considered a PEP. The bank may, within its policies and procedures, set specific criteria to consider a local person a PEP.

3-8 Reporting Officer
The officer directly responsible for the anti-money laundering and counter-terrorist financing program at the bank, as defined by the System for Monitoring Operations issued under Decision No. 19 of 2019. This officer manages and heads the compliance verification unit. This task is undertaken by the Manager of the Compliance Monitoring Department at the bank.

3-9 Compliance Verification Unit:
The unit responsible for verifying the bank's compliance with anti-money laundering and counter-terrorist financing requirements and procedures within the banking and financial institution, headed by the Head of the Compliance Verification Unit.

3-10 Compliance Monitoring Department:
An independent department reporting to the bank's Board of Directors, responsible for ensuring the bank's compliance with all applicable laws and regulations governing banking work in the Syrian Arab Republic, particularly those related to anti-money laundering and counter-terrorist financing procedures. It was renamed by the Credit and Money Council Decision No. 1468 / M N A B 4 for the year 2016, merging the functions of the Reporting Officer, internal banking auditor, and compliance monitoring.

3-11. Permanent Business Relationship:
A relationship that, upon establishment, is expected to last for a relatively long period. This includes, but is not limited to, creditor or debtor bank accounts, facilities of any type, financial leasing contracts, credit and payment card contracts, or life insurance or investment-oriented insurance product contracts.

3-12. Occasional Business Relationship or Transaction
A business relationship that, upon establishment, is not expected to last for a relatively long period, or that represents a single banking or financial operation where the relationship ends upon its completion. For example, executing a single transfer, a single foreign exchange operation, a cash deposit into an account of one of the bank's clients by a third party, or the cash collection of a cheque or payment order drawn by one of the bank's clients.

3-13 Beneficial Owner
The natural person who is the true beneficiary of the relationship between the bank and the customer. In other words, the true beneficiary of the banking operation. This includes natural persons who own the legal entity (company, etc.) and exercise ultimate effective control over it.

3-14. National Risk Assessment of Money Laundering and Terrorist Financing
Refers to the report identifying and assessing money laundering and terrorist financing risks at the national level in the Syrian Arab Republic, which the Authority prepares at least once every three years in coordination with relevant parties, as stipulated in the executive instructions.

2-19 Originating Banking and Financial Institution: The banking and financial institution that initiates the transfer and moves funds or value upon receiving a transfer order on behalf of the ordering customer.

2-20 Intermediary Banking and Financial Institution: The banking and financial institution in the payment chain that receives and transmits the transfer on behalf of the originating banking and financial institution and the beneficiary banking and financial institution or another intermediary banking and financial institution.

2-21 Beneficiary Banking and Financial Institution: The banking and financial institution that receives the transfer from the originating banking and financial institution directly or through an intermediary banking and financial institution and provides the funds or value to the beneficiary.
2-22 Ordering Customer: Refers to the natural or legal person who issues the transfer order through the originating banking and financial institution to execute the transfer.
2-23 Correspondent Payable-Through Accounts: Refer to correspondent accounts used directly by third parties to conduct business on their own behalf.
2-24 Reasonable Measures: Measures proportionate to the money laundering or terrorist financing risks associated with the nature of the customer or the operation.
2-25 Unique Identifier: A code consisting of a mix of letters, numbers, or symbols referring to a specific transfer, defined according to the message system protocols used in the transfer.
2-26 High-Risk Accounts: Accounts that carry a high risk of being used for money laundering or terrorist financing operations. For example, accounts of exchange companies, internal transfer companies, charitable associations, as well as accounts of lawyers, certified accountants, and gold and jewelry dealers are considered high-risk accounts.
2-27 System for Monitoring Banking Operations: The System for Monitoring Banking and Financial Operations in banking and financial institutions operating in the Syrian Arab Republic and the Syrian free zones for the purpose of combating money laundering and terrorist financing, issued in 2019 by Decision /19/.

II - Basic Principles of Anti-Money Laundering and Counter-Terrorist Financing at the Bank:

Principle One: Responsibility of Cham Bank's Board of Directors: The bank's Board of Directors is primarily responsible for compliance with Legislative Decree /33/ of 2005, its amendments, its executive instructions, and the System for Monitoring Operations stipulated in Decision No. /19/ for the year 2019 and its amendments.

Principle Two: Establishing and Implementing the AML/CTF Program: The bank's Board of Directors is committed to adopting an anti-money laundering and counter-terrorist financing program prepared by the executive management. This program must be proportionate to the money laundering and terrorist financing risks borne by Cham Bank, and the size, nature, and complexity of its operations, and must be compatible with the requirements of Legislative Decree /33/ of 2005, its amendments, its executive instructions, and the System for Monitoring Operations stipulated in Decision No. 19 / of 2019 and its amendments.

Principle Three: Compliance Arrangements: Cham Bank's Board of Directors is committed to working on approving compliance arrangements, including appointing a Reporting Officer and forming a unit to verify compliance with the procedures, laws, and regulations related to combating money laundering and terrorist financing.

Principle Four: Customer Due Diligence: Cham Bank is committed to exercising customer due diligence in accordance with the requirements of Legislative Decree /33/ of 2005, its amendments, its executive instructions, and the System for Monitoring Operations stipulated in Decision No. /19/ for the year 2019 and its amendments.

Principle Five: Reporting Suspicious Transactions and Funds: The bank's Reporting Officer is committed to reporting suspicious transactions and funds in accordance with the requirements of Legislative Decree /33/ of 2005, its amendments, its executive instructions, and the System for Monitoring Operations stipulated in Decision No. /19/ for the year 2019 and its amendments.

Principle Six: Cooperation with the Authority: Cham Bank is committed to fulfilling all requests for information and data from the Authority and cooperating with it when requested by all levels of the bank.

Principle Seven: Appointment and Training Standards: Cham Bank is committed to high standards when appointing or employing staff and officials. It is also committed to developing a continuous and appropriate training program on anti-money laundering and counter-terrorist financing for its officials and employees.

Principle Eight: Demonstrating Compliance: Cham Bank is committed to providing all evidence and documents confirming its compliance with the requirements of Legislative Decree /33/ for the year 2005, its amendments, its executive instructions, and the System for Monitoring Operations stipulated in Decision No. /19/ for the year 2019 and its amendments, upon request by the Authority and the relevant supervisory bodies.

III - Assessment of Money Laundering and Terrorist Financing Risks:

Cham Bank follows the following steps at least every four years to conduct a risk assessment related to money laundering and terrorist financing:

a. Understanding the internal and external environment in which the bank operates:

1. When understanding internal factors, factors related to the bank's size, particularly the size of its assets and customer base, its structure, risk and compliance culture, and the level of available resources, especially human and IT resources, and the impact of these factors on money laundering and terrorist financing risks are considered.
2. When understanding external factors, factors related to current or potential major criminal threats it may face, and various political, social, and economic factors are considered. The National Risk Assessment of Money Laundering and Terrorist Financing can be relied upon for this.

b. Identifying the categories of customers, products, service delivery channels, and countries and geographical locations where Cham Bank operates or deals with, or to which its current or potential customers belong, which could pose money laundering and terrorist financing risks or could be exploited for such purposes.

c. Assessing current or potential individual and entity customers, where categories of customers, legal persons, and entities that may pose higher risks should be identified based on the nature of their business, customer functions, or the nature of expected transaction activity.

d. Assessing current or potential products and services, where banking products and services that may pose a higher risk for money laundering or terrorist financing should be identified.
e. Assessing current or potential banking service delivery channels, where channels that may pose higher risks for money laundering or terrorist financing should be identified.
f. Assessing countries and geographical locations where Cham Bank is present or will be present, where its current or potential customers or support service providers are located, and those with which it deals or will deal. Local and international geographical locations that may pose a higher risk in the field of money laundering and terrorist financing should be identified.
g. Detailed analysis of data related to Cham Bank's customer categories, products, service delivery channels, and countries and locations, and those obtained during the customer identification and verification phase, in order to evaluate this data.

Identifying and Assessing Risks of Legal Persons, Legal Arrangements, and Non-Profit Organizations

a. Risks posed by legal persons and legal arrangements must be identified, assessed, and documented, particularly those arising from reduced transparency or an increased ability to conceal risks.
b. Cham Bank should ensure that risks arising from beneficial owners, guardians, settlors, beneficiaries, directors, or any other related entities are reflected in the risk characterization of legal persons and legal arrangements.
c. Within the framework of identifying, understanding, and assessing the risks of non-profit organizations, Cham Bank should take into account the money laundering and terrorist financing risks posed by relationships with this type of customer and their various areas of activity.

New Business Products and Practices:

Cham Bank is committed to identifying, understanding, and assessing money laundering or terrorist financing risks that may arise from:

1. Developing new business products and practices, including new service delivery channels or distribution mechanisms.
2. Using or developing new technologies for both new and existing products.
3. This risk assessment must be conducted before launching new products or business practices, or using or developing new technologies. In this case, Cham Bank is committed to taking appropriate measures to manage and mitigate those risks.

Ensuring the Effectiveness of AML/CFT Systems in Other Countries and Geographical Locations

a. During the process of identifying, understanding, and assessing risks, and when evaluating the effectiveness of anti-money laundering systems in other countries and geographical locations, Cham Bank considers the following factors:

1. The legal framework.
2. The effectiveness of supervision and oversight of banking and financial institutions in these countries.
3. International cooperation.

4. b. Within this assessment, Cham Bank considers available information on anti-money laundering systems in other countries published by relevant entities, such as mutual evaluation reports issued by the FATF and similar regional groups.

IV- Responsibilities of Various Parties within the Framework of the AML/CTF Program at Cham Bank:

1. Responsibilities of the Board of Directors:
The Bank's Board of Directors is responsible for approving the anti-money laundering and counter-terrorist financing program, including the related policies, procedures, and controls. It ensures the following:
1-1. Reviewing reports on the assessment, identification, and understanding of money laundering and terrorist financing risks at the bank, and making all decisions required by the results of this review, including decisions related to developing the AML/CTF program according to these reports.
1-2. Approving the AML/CTF program in all its components, and following up on its periodic evaluation and making decisions accordingly.
1-3. Determining the reports that should be submitted by the Reporting Officer, the Compliance Verification Unit, and the Executive Management, and their timelines, to enable the Board of Directors to fulfill its responsibilities.
1-4. Monitoring the bank's risk management concerning AML/CTF by providing continuously updated and timely information and taking appropriate measures accordingly.
1-5. Working to deepen the culture of combating money laundering and terrorist financing within the bank.
1-6. Exercising all other tasks assigned to the Bank's Board of Directors regarding combating money laundering and terrorist financing under the Legislative Decree, its executive instructions, and the System for Monitoring Operations issued under Decision No. 19 / of 2019.

2. Responsibilities of the Executive Management:
The Executive Management at the bank, at every level of the bank, its departments, and branches, is responsible for implementing the policies, procedures, and controls related to combating money laundering and terrorist financing. In this framework, the Executive Management does the following:

a. Providing all information needed by the Compliance Verification Unit, through all the bank's directorates, departments, and branches, and at all administrative levels, which assists in preparing reports on the assessment, identification, and understanding of money laundering and terrorist financing risks at the bank.
b. Proposing policies, procedures, and controls for combating money laundering and terrorist financing, in a manner that achieves compliance with the Legislative Decree, its executive instructions, and the System for Monitoring Operations issued under Decision No. 19 / of 2019, and addresses the identified, understood, and assessed money laundering and terrorist financing risks, in coordination with the Reporting Officer and the Compliance Verification Unit. These policies, procedures,

regulations, and controls are to be approved by the Board of Directors and integrated into the bank's operational manuals.

c. Monitoring the application of policies, procedures, and controls for combating money laundering and terrorist financing in all directorates, departments, and branches of the bank, and at all administrative levels, and raising reports thereon to the Board of Directors.
d. Periodic review of the effectiveness of policies, procedures, and controls for combating money laundering and terrorist financing and recommending their amendment to the Board of Directors if necessary.
e. Proposing, designing, and implementing continuous training programs regarding anti-money laundering and counter-terrorist financing for officials and employees of the bank in coordination with the Reporting Officer and the Compliance Verification Unit, and monitoring their implementation at all levels of the bank, its directorates, departments, and branches.
f. Providing information and assistance that the Reporting Officer and the Compliance Verification Unit may need.
g. Exercising all other tasks assigned to the Executive Management in the bank regarding combating money laundering and terrorist financing under the Legislative Decree, its executive instructions, the System for Monitoring Operations issued under Decision No. /19/ for the year 2019, and the AML/CTF program.

3. Responsibilities of the Reporting Officer:

The Reporting Officer and the Compliance Verification Unit undertake the following:

3-1. The Reporting Officer exercises money laundering and terrorist financing risk management and prepares, supervises, the related policies, procedures, regulations, and controls through the following tasks:

3-1-1. Supporting and coordinating the work of the Board of Directors and the Executive Management in managing the bank's risks associated with combating money laundering and terrorist financing.

3-1-2 Participating in preparing reports on the assessment, identification, and understanding of money laundering and terrorist financing risks.

3-1-3. Proposing policies, procedures, and controls for combating money laundering and terrorist financing, in a manner that achieves compliance with Legislative Decree No. 33, its executive instructions, and Decision /19/, and addresses the identified, understood, and assessed money laundering and terrorist financing risks, in coordination with the Executive Management. These policies, procedures, regulations, and controls are to be approved by the Board of Directors.

3-1-4 Periodic review of the effectiveness of policies, procedures, and controls for combating money laundering and terrorist financing, and recommending their amendment to the Board of Directors.

3-1-5. Follow-up and supervision of the application of anti-money laundering and counter-terrorist financing policies, procedures, and controls in the bank in coordination with the Executive Management.

3-1-6. Reviewing internal and external audit reports regarding compliance with anti-money laundering and counter-terrorist financing policies, procedures, and controls, and all other reports related to compliance with anti-money laundering and counter-terrorist financing procedures.

3-1-7. Submitting reports to the Board of Directors on matters related to combating money laundering and terrorist financing.

3-1-8. Monitoring the accountability process regarding non-compliance with anti-money laundering and counter-terrorist financing policies, procedures, and controls in the bank.

3-2. The Reporting Officer exercises ongoing monitoring of operations and suspicious transaction reports through the following:

3-2-1. Receiving, processing, and evaluating suspicious transaction reports.

3-2-2. Reviewing periodic and non-periodic reports received from concerned directorates and branches regarding all accounts and banking and financial operations, such as transfer and cash operation reports.

3-2-3. Monitoring customer accounts and operations, according to a risk-based approach, in a way that helps detect unusual operations.

3-2-4. Preparing suspicious transaction reports and submitting them to the Authority.

3-2-5. Acting as a point of contact between Cham Bank and the Authority, the competent supervisory body, and other official bodies regarding anti-money laundering and counter-terrorist financing matters.

3-2-6. Responding immediately to requests for information received from the Authority regarding anti-money laundering and counter-terrorist financing.

3-3. Regarding other tasks:

Exercising all other tasks assigned to the Reporting Officer and the Compliance Verification Unit under Legislative Decree No. 33 of 2005, its executive instructions, and Decision No. 19 / of 2019 and its amendments.

3-4. Reports Submitted to the Board of Directors by the Reporting Officer

3-4-1. The Reporting Officer is committed to submitting a report to the Board of Directors at least twice a year, containing an assessment of the adequacy and effectiveness of the policies, procedures, and controls related to combating money laundering and terrorist financing, including the following details:

3-4-1-1 The reality of money laundering and terrorist financing risks at the bank through the money laundering and terrorist financing risk assessment, identification, and understanding report and its updates and changes.

3-4-1-2 The reality of the implementation of the anti-money laundering and counter-terrorist financing program at the bank, including policies, procedures, regulations, and controls.

3-4-1-3 Gaps in the anti-money laundering and counter-terrorist financing program and points for improvement in the policies, procedures, regulations, and controls related to combating money laundering and terrorist financing in light of the risks faced by the bank.

3-4-1-4 Violations committed against Legislative Decree No. 33 of 2005, its executive instructions, Decision /19/ of 2019, and relevant anti-money laundering policies, procedures, and administrative instructions.

3-4-1-5 Training on anti-money laundering and counter-terrorist financing provided to employees at all levels in the bank and evaluation of results and suggestions for improvement.

3-4-1-6 The number and nature of internal suspicious transaction reports submitted and the number of suspicious transaction reports submitted to the Authority.

3-4-1-7 Progress in following up on observations from the review of the previous report by the Board of Directors, internal and external evaluation reports, supervisory bodies' reports, and action plans to address the deficiencies indicated in these reports.

3-4-2. If the report identifies deficiencies in the bank's anti-money laundering and counter-terrorist financing program and its compliance with the Legislative Decree, its executive instructions, and Decision No. /19/ and its amendments, the Board of Directors must approve an action plan prepared in coordination between the Compliance Verification Unit and the Executive Management and documented to address the deficiencies in a timely manner.

3-4-3 The Reporting Officer is committed to sending a copy of the report and the aforementioned action plan to the Authority.

3-5 Qualifications of the Reporting Officer:

The Reporting Officer in banking institutions is appointed by a decision issued by the Management Committee of the Anti-Money Laundering and Counter-Terrorist Financing Authority, subsequent to the Credit and Money Council decision appointing them as Manager of the Compliance Monitoring Department after nomination by the bank's Board of Directors.

3-5-1. The Reporting Officer must meet the following conditions and qualifications:

3-5-1-1 A university degree in one of the fields of financial, economic, or legal sciences.

3-5-1-2 Practical experience in the banking or financial field of not less than five years. An exception from this condition may be granted, on a case-by-case basis, by the Authority's Management Committee.

3-5-1-3 Good skills in the English language and computer use.

3-5-1-4 Conditions that must be met by employees working in the bank.

3-5-1-5 Conditions for foreign employment if the candidate is not a Syrian Arab national or considered as such.

3-5-1-6. Integrity and the ability to perform his duties objectively and independently, especially when processing internal suspicious transaction reports and responding to information requests from the Authority.

3-5-2. The Reporting Officer must have the following:

3-5-2-1 A high administrative level and the necessary powers to perform his work according to sound professional and ethical standards and according to the requirements of this system.

3-5-2-2 Free and timely access to all information in the bank, including:

1. All customer data and documents obtained within the framework of the due diligence process and their accounts and operations, including holders of numbered accounts in banks, especially identification and verification documents.
2. All transaction records.

3-5-2-3 The right to communicate with the Board of Directors and its committees and the Executive Management in the bank.

3-5-2-4 The right to direct contact, within the framework of his duties, with the Anti-Money Laundering and Counter-Terrorist Financing Authority, the competent supervisory bodies, or with other official bodies and their employees.

3-5-3. The Compliance Verification Unit must be provided with appropriate and sufficient resources, staff, and technologies to perform its role effectively, objectively, and independently. The employees in the Compliance Verification Unit should possess diverse qualifications and experiences appropriate to the tasks assigned to it.

3-4-1-7 Progress in following up on observations from the review of the previous report by the Board of Directors, internal and external evaluation reports, supervisory bodies' reports, and action plans to address the deficiencies indicated in these reports.

3-4-2. If the report identifies deficiencies in the bank's anti-money laundering and counter-terrorist financing program and its compliance with the Legislative Decree, its executive instructions, and Decision No. /19/ and its amendments, the Board of Directors must approve an action plan prepared in coordination between the Compliance Verification Unit and the Executive Management and documented to address the deficiencies in a timely manner.

3-4-3 The Reporting Officer is committed to sending a copy of the report and the aforementioned action plan to the Authority.

3-5 Qualifications of the Reporting Officer:

The Reporting Officer in banking institutions is appointed by a decision issued by the Management Committee of the Anti-Money Laundering and Counter-Terrorist Financing Authority, subsequent to the Credit and Money Council decision appointing them as Manager of the Compliance Monitoring Department after nomination by the bank's Board of Directors.

3-5-1. The Reporting Officer must meet the following conditions and qualifications:

3-5-1-1 A university degree in one of the fields of financial, economic, or legal sciences.

3-5-1-2 Practical experience in the banking or financial field of not less than five years. An exception from this condition may be granted, on a case-by-case basis, by the Authority's Management Committee.

3-5-1-3 Good skills in the English language and computer use.

3-5-1-4 Conditions that must be met by employees working in the bank.

3-5-1-5 Conditions for foreign employment if the candidate is not a Syrian Arab national or considered as such.

3-5-1-6. Integrity and the ability to perform his duties objectively and independently, especially when processing internal suspicious transaction reports and responding to information requests from the Authority.

3-5-2. The Reporting Officer must have the following:

3-5-2-1 A high administrative level and the necessary powers to perform his work according to sound professional and ethical standards and according to the requirements of this system.

3-5-2-2 Free and timely access to all information in the bank, including:

1. All customer data and documents obtained within the framework of the due diligence process and their accounts and operations, including holders of numbered accounts in banks, especially identification and verification documents.
2. All transaction records.

3-5-2-3 The right to communicate with the Board of Directors and its committees and the Executive Management in the bank.

3-5-2-4 The right to direct contact, within the framework of his duties, with the Anti-Money Laundering and Counter-Terrorist Financing Authority, the competent supervisory bodies, or with other official bodies and their employees.

3-5-3. The Compliance Verification Unit must be provided with appropriate and sufficient resources, staff, and technologies to perform its role effectively, objectively, and independently. The employees in the Compliance Verification Unit should possess diverse qualifications and experiences appropriate to the tasks assigned to it.

4. Responsibilities of the Operations Monitoring Officer in Branches:

4-1. An Operations Monitoring Officer in the branch is appointed by the Executive Management of the bank based on the proposal of the Reporting Officer in each governorate of the country, except for the capital, where the appointment is made for every three branches or less that are geographically close.

4-2. The Operations Monitoring Officer in the branch reports to the Reporting Officer. The bank may assign him non-executive work alongside his primary function, after obtaining the approval of the Reporting Officer and under his responsibility.

4-3. Operations Monitoring Officers at the branch level perform the following tasks:

4-3-1. Verifying the compliance of officials and workers in the branches with the bank's anti-money laundering and counter-terrorist financing program and with the Legislative Decree, its executive instructions, and the System for Monitoring Operations issued under Decision No. /19/ of 2019.

4-3-2 Monitoring customer accounts and operations at the bank, according to a risk-based approach, in a way that helps detect suspicious operations.

4-3-3 Notifying the Compliance Verification Unit of any suspicious operations and the extent of the branches' adherence to the required procedures.

V: Anti-Money Laundering and Counter-Terrorist Financing Program

Cham Bank should establish an adequate and effective anti-money laundering and counter-terrorist financing program that is proportionate to its money laundering and terrorist financing risk assessment. This program should be reviewed by the bank's management at least every two years. This program consists of:

1. Compliance arrangements, including the appointment of a Reporting Officer and the formation of a verification unit.
   Within the framework of its commitment to compliance arrangements, the bank has formed a Compliance Monitoring Department and a Compliance Verification Unit for anti-money laundering and counter-terrorist financing procedures, which requires creating the position of Reporting Officer. Cham Bank is committed to appointing a Reporting Officer according to the appointment requirements stipulated in Decision No. 19 of 2019 and enabling him with all the powers stipulated in Decision No. 19 to perform his duties optimally.
   On the other hand, the bank forms a unit to verify the bank's compliance with anti-money laundering and counter-terrorist financing procedures and staffs it with sufficient and qualified personnel to carry out the tasks assigned to it.
2. Developing and implementing internal policies, procedures, and controls for combating money laundering and terrorist financing, including at a minimum:
   - Customer acceptance policies.
   - Due diligence measures.
   - Record preparation and retention.
   - Ongoing monitoring and detection of suspicious transactions.
   - Internal and external reporting requirements.

* Implementation of freezes issued by the Authority and relevant parties.
* Any other matters that may be required by Legislative Decree No. 33 of 2005 and its amendments, its executive instructions, or the System for Monitoring Operations issued under Decision No. 19 / of 2019 and its amendments, as applicable and according to what applies to Cham Bank.

3. Having high standards for hiring employees through appropriate vetting procedures.
4. Establishing a continuous training program on anti-money laundering and counter-terrorist financing procedures, including disseminating a culture of compliance with anti-money laundering and counter-terrorist financing.
5. An independent internal or external audit function.

Customer Acceptance Policies

1-1. All employees of branches and departments concerned with direct customer interaction, at all job levels, must not accept dealing with any customer, whether permanent or occasional, by opening an account, granting any banking facilities, or performing any banking services, without clearly identifying them, knowing their economic activity, determining the beneficial owner who effectively controls the account or the operation being conducted, and knowing if the customer holds any other nationality or residency in another country when establishing a permanent business relationship.

1-2. Each customer of Cham Bank maintains only one account and cannot open another account for any reason. However, it is possible for them to have a personal account, a joint account, and a partnership account at the same time.

1-3. Opening numbered accounts (accounts where the customer's identity is not displayed for any reason) is prohibited. If there is any need for such accounts, a written request must be submitted by the Branch Management Department Manager, attached with all customer identification documents, after providing his recommendations to the Chief Executive Officer.

1-4. The branch keeps a copy of the identification document signed by the bank employee stating that it is a true copy.

1-5. The bank does not accept dealing with customers proven to be involved in illegal cases.

1-6. Dealing with persons and entities listed in the lists of terrorists circulated by Prime Minister's Decision No. 851 dated 13/3/2014 and its amendments is prohibited. It is obligatory to verify that no new accounts are opened for those listed by using the program utilized by the Verification Unit. Dealing with any natural or legal person whose name has been circulated by the Anti-Money Laundering and Counter-Terrorist Financing Authority within the lists of prohibited persons is also prohibited, unless otherwise indicated by the Authority.

1-7. Accounts opened electronically are dealt with according to decisions issued by the regulatory authorities and may be converted to regular accounts based on the customer's desire if they come to one of the branches and provide the documents and sign the required documents for a regular account.

1-8. Verifying information provided by customers, and if unable to do so, dealing with the customer must not be accepted.

1-9. The policy for accepting natural persons applies to customer agents and those authorized by them.
1-10 In general, when accepting any customer or opening a new account, the content of the administrative instructions approved by Cham Bank regarding the mechanism for opening accounts and identification documents for each type of customer, whether a natural or legal person, must be adhered to.
1-11 All bank customers are classified according to money laundering and terrorist financing risks. Specific risk factors are applied to assess the degree of customer risk regarding money laundering and terrorist financing operations through the program utilized in the bank. Each customer is given a risk rating ranging from (Low - Medium - High) based on a number of indicators, which are:

- Nationality
- Economic sector (business sector).
- Types of transactions
- Currencies
- City or geographical region.
- Type of customer

Other factors (the presence of any of these makes the final classification high) and include:

- Subject of inquiry by the Authority
- Name on blacklists
- Beneficiary is not the account holder
- Non-resident

The final classification for the account is given based on the sum total of these previous factors according to the formula entered into the program.
The classification given to each account is not considered final, as it is possible to raise or lower the classification degree from low to medium or high, or vice versa, based on the data resulting from ongoing monitoring procedures of operations.
1-12 When a permanent business relationship exists between the customer and the bank, executing any occasional transaction outside the framework of the permanent business relationship is prohibited, except in the following cases:

a. When the occasional transaction does not exceed one million Syrian pounds or its equivalent in foreign currencies, and this limit is subject to amendments approved by the Anti-Money Laundering and Counter-Terrorist Financing Authority.
b. When the customer is not a direct party in another business relationship on behalf of others (agent, authorized person, guardian, authorized signatory, company employee, etc.). The responsibility for determining whether the customer is a direct or indirect party lies with the branch executing the transaction.

Due Diligence Measures:

- All business relationships, including numbered bank accounts, and occasional business relationships or transactions at Cham Bank are subject to customer due diligence procedures, according to the Legislative Decree, its executive instructions, and Decision No. 19 of 2019 issued by the Authority and its amendments.

- Dealing with anonymous customers or those using pseudonyms is prohibited. Likewise, commencing business relationships with anonymous parties or under fictitious names is prohibited.
- Commencing any business relationship is prohibited unless the customer's identity and activity are identified and verified, the beneficial owner is determined, and the procedures applied at Cham Bank are used to verify their identity, according to the requirements of the decisions, laws, and administrative instructions approved by the bank and using the specified official documents. Likewise, commencing any business relationship is prohibited before obtaining information regarding the purpose of the business relationship and its intended nature and understanding this purpose. Reasonable measures should also be taken to find out if the customer holds any other nationality or residency in another country when establishing a permanent business relationship.
- If the relationship with the customer is built, ongoing monitoring is exercised regarding the business relationship, and the business conducted by the customer during the duration of this relationship is audited and assessed regularly, to ensure that the operations conducted during the course of the business relationship are consistent with the information held by the bank about the customer, their activity, risk nature, and source of funds.
- When identifying the beneficial owner in the business relationship:
  1. Cham Bank must determine for all customers whether the customer is acting on behalf of another person. All necessary steps must be taken to obtain sufficient identification data to verify the identity of that other person.
  2. Regarding legal persons or legal arrangements, the nature of the customer's business, ownership structure, and nature of control should be understood. In addition, the natural person or persons who have ownership or control over the customer should be identified.
- If due diligence procedures cannot be carried out, the bank must not commence the business relationship or conduct the operations, or terminate the business relationship, and the case must be raised to the Reporting Officer at the bank for study and consideration of submitting a report on a suspicious transaction to the Authority.
- In case of suspicion of money laundering or terrorist financing, a suspicious transaction report can be submitted without completing the due diligence procedures to avoid alerting the customer.

Requirements for the Extent of Application of Due Diligence Procedures

a. The extent of enhancement of the measures taken regarding customer due diligence, including ongoing monitoring, is decided based on the risk characterization of the business relationship. Enhanced due diligence measures should be taken in high-risk business relationships, and simplified due diligence measures should be taken in low-risk business relationships.

b. The risk characterization of the business relationship is based on multiple factors, including customer risk, product risk, service delivery channel risk, and country and geographical region risks. This characterization is updated to consider all changes that occur in the business relationship.

c. Cham Bank should be in a position to demonstrate to the competent supervisory body and the Authority that the extent of application of customer due diligence measures is appropriate and proportionate to the associated money laundering and terrorist financing risks.

The types of customers listed below, for example but not limited to, may require enhanced due diligence measures, including ongoing monitoring:

- Customers legally subject to anti-money laundering and counter-terrorist financing procedures (financial institutions or designated non-financial businesses and professions - DNFBPs).
- Bank accounts belonging to customers found to be missing, absent, or kidnapped.
- Professions primarily based on cash (restaurants, nightclubs, car dealers, transport and shipping companies, travel and tourism offices, institutions authorized by the General Postal Corporation to provide postal services).
- Politically Exposed Persons (PEPs).
- Non-profit organizations.
- Companies and individuals working in the Syrian free zones.
- Companies and individuals working in countries known to be tax havens.
- Non-face-to-face customers.
- Non-resident customers.
- Customers with wealth of unknown source.
- Customers who deal through agents or intermediaries without justification.
- Companies with capital wholly or partly composed of bearer shares.
- Customers whose business typically requires sending and receiving high-value transfers exceeding ten thousand US dollars or equivalent (import and export.... etc.)
- Customers who deal in large cash amounts even though their activity does not belong to cash-intensive activities.
- Customers with multiple business relationships with the same banking and financial institution or with other banking and financial institutions located in the same area, without a clear purpose.
- Customers whose operations or funds have been reported to the Anti-Money Laundering and Counter-Terrorist Financing Authority on suspicion of concealing money laundering or terrorist financing, or whose funds are suspected to be proceeds of one of the crimes listed in paragraph (c) of Article One of the Legislative Decree, or related to terrorism, or used by terrorists or terrorist organizations or those who finance terrorism...

The banking services listed below, for example but not limited to, necessitate the application of enhanced due diligence measures, including ongoing monitoring:

- Use of payable-through accounts.
- Electronic banking and financial services.
- Foreign exchange.
- Transfers.
- Cheques.

- Local and international private banking services.
- Financial instruments.
- Safe deposit boxes.
- Correspondent relationships.
- Foreign exchange accounts.
- Documentary credits.
- Bills for collection.
- Lending activities secured by deposit accounts and cash guarantees and securities.

Business conducted through one of the following channels is an example of business that requires enhanced due diligence measures due to being conducted using modern technologies and not face-to-face:

- Various types of relationships and operations concluded via the Internet, cellular networks, or other advanced technical means.
- Services or operations provided or conducted via the Internet, cellular networks, use of ATMs, etc.
- Electronic point-of-sale transactions, or use of pre-paid, reloadable, or account-linked cards.

Countries and geographical regions belonging to one of the following categories require enhanced due diligence measures:

- Countries and geographical regions where anti-money laundering and counter-terrorist financing systems are ineffective.
- Countries and geographical regions with deficiencies in international cooperation.
- Countries and geographical regions with high levels of corruption.
- Countries and geographical regions with high crime rates, particularly related to drug trafficking.

a. Simplified due diligence measures, including ongoing monitoring, may be applied for the following types of customers:

1- Government economic institutions and companies.
2- Public administrations or institutions.
3- Companies listed on the stock market and subject to disclosure requirements (either through stock market rules, law, or any mandatory means).

b. Simplified due diligence measures may be applied for the following types of services and service delivery channels, including ongoing monitoring:

1- Financial services or products targeting specific types of customers, such as employees or university students, to increase financial inclusion opportunities.

c. Simplified due diligence measures may be applied for countries and geographical regions belonging to any of the following categories:

1- Countries identified by reliable sources, such as mutual or joint evaluation reports or detailed evaluation reports issued by the FATF or similar regional groups like the Middle East and North Africa FATF (MENAFATF), as having effective anti-money laundering and counter-terrorist financing systems.
2- Countries identified by reliable sources as having low levels of corruption or other criminal activities.

d. Cham Bank is committed to taking into account risk variables associated with risk categories related to types of customers, products, service channels, and countries or geographical regions when deciding the extent of enhancement of the measures it will take regarding customer due diligence. These variables, whether individually or collectively, can increase or reduce the potential risk, which in turn is reflected in the appropriate level of due diligence. Examples of these variables include:

1. The purpose of the account or relationship.
2. The level of assets deposited by a customer or the volume of operations conducted.
3. The regularity or duration of the business relationship.

e. Cham Bank is committed to taking into account potential changes in money laundering and terrorist financing risk between different regions within the territories of the Syrian Arab Republic when deciding the extent of enhancement of the measures it will take regarding customer due diligence.

f. The existence of a low risk for money laundering and terrorist financing at the identification and verification stage does not automatically mean that the customer himself is low risk for all types of due diligence measures, especially in the case of ongoing monitoring of operations.

Enhanced and Simplified Due Diligence Procedures

a. When the money laundering or terrorist financing risks associated with a customer or a business relationship are high, enhanced due diligence measures are applied, consistent with the identified risks. In particular, the degree and nature of monitoring of the business relationship should be increased to determine whether those operations or activities appear unusual or suspicious. Following are examples of enhanced due diligence measures that can be applied to high-risk business relationships:

1- Obtaining additional information about the customer, and updating customer and beneficial owner identification data regularly and frequently.

2- Obtaining additional information about the expected nature of the business relationship.

3- Obtaining information about the source of funds or the source of the customer's wealth.

4- Obtaining information about the reasons for expected or conducted operations.

5- Obtaining approval from senior executive management to start or continue the business relationship.

6- Applying enhanced monitoring of the business relationship, by increasing the number and timing of controls, and selecting patterns of operations that require more scrutiny and review.

b. When the money laundering or terrorist financing risks associated with a customer or a business relationship are low, Cham Bank may apply simplified due diligence measures, which should take into account the nature of these low risks. The simplified measures should be proportionate to the low risk factors. For example, simplified measures may relate only to customer acceptance procedures or ongoing monitoring). Following are examples of measures that can be taken:

1- Verifying the identity of the customer and the beneficial owner after establishing the business relationship.

2- Reducing the frequency of customer identification update processes.

3- Reducing the degree of ongoing due diligence and auditing of operations based on an acceptable cash threshold level.

4- Not collecting specific information or implementing specific procedures to understand the nature and purpose of the business relationship, but inferring them from the type of operations conducted or the existing business relationship.
Simplified due diligence measures are not acceptable when there is suspicion of money laundering or terrorist financing, or when specific high-risk scenarios materialize.

Timing of Due Diligence Procedures:

a. Customer due diligence procedures are implemented when:

1. Before or during the establishment of a permanent business relationship or during a business relationship or an occasional transaction or several linked occasional transactions.
2. There is suspicion that a customer is attempting to conduct money laundering or terrorist financing operations, regardless of any exemptions or specific limits.
3. There is doubt about the accuracy or adequacy of previously obtained data.
4. Subsequent changes occur in the identity and activity of the customer or the identity of the authorized signatory or the identity of the beneficial owner of an existing business relationship or account.
5. A material change occurs in the way an account at the bank is operated or material changes in the manner of managing the business relationship.

b. The customer verification process can be completed after establishing the business relationship, provided that this is done within a reasonable time not exceeding 10 working days, it is necessary to avoid interrupting normal business flow, and money laundering and terrorist financing risks are effectively managed.

c. When allowing verification to be completed after establishing the business relationship, risk management procedures associated with the conditions under which the customer can benefit from the relationship before verification must be adopted. This should include a set of measures, such as restrictions on the number, types, and/or amount of transactions that can be conducted, and tracking large or complex transactions that exceed the expected standards for this type of relationship.

d. Due diligence procedures for existing customers are implemented based on materiality and risk. Due diligence should be implemented in such existing relationships at appropriate times, taking into account whether due diligence procedures have been previously applied to customers and when they were applied, as well as the adequacy of the information obtained.

5. Politically Exposed Persons (PEPs)

5-1 They are persons who hold any of the following positions in a foreign country:

5-1-1 Head of State and his advisors, deputies, and heads of presidential institutions.

5-1-2 Prime Minister and members of the Council of Ministers and their equivalents.

5-1-3 Directors of security branches and apparatuses and senior officials therein in administration and branches.

5-1-4 Leaders and senior officials of political parties and holders of important positions therein.

5-1-5 Ambassadors, consuls, and members of the diplomatic corps.

5-1-6 Heads and directors of international organizations, their deputies, and representatives.

5-1-7 Brigade leaders and senior army officers.

5-2 These categories are identified through profession proof documents according to the requirements of Decision /19/ related to profession proof and the administrative instructions specific to the approved account opening guide.
5-3 Relevant websites on the Internet can also be consulted to identify these persons or to verify if a specific person is a PEP or not.
5-4 An account cannot be opened for any of the aforementioned persons before obtaining the approval of the Chief Executive Officer or his delegate, likewise regarding continuing an already open account whose holder later falls within those categories.
5-5 Accounts opened as such are subject to enhanced due diligence measures as mentioned in this guide.
5-6 Taking reasonable measures to know the source of wealth or source of funds of customers and beneficial owners who have been identified as PEPs.
5-7 In case of encountering any situation where it is difficult to determine the nature of the customer and their affiliation with one of the mentioned categories is likely, the case must be presented to the Reporting Officer.
5-8 Enhanced due diligence measures also apply to domestic PEPs and local persons assigned prominent positions by an international organization if it is found that the business relationship with them carries high risks.
5-9 If it is discovered later that a current customer or beneficial owner is a PEP, or if the customer or beneficial owner becomes a PEP, the bank may continue the relationship with them, but after approval from senior management.
5-10 The bank applies the requirements for all types of PEPs to their family members or close associates.

6. Exchange Companies and Internal Transfer Companies In addition to the customer due diligence procedures mentioned earlier in this guide, the bank is committed to the following:
6-1 No account is opened for an exchange company or transfer company without prior approval from the Compliance Verification Unit, even if previous business relationships exist. The purpose of opening the account and the need of the exchange company or internal transfer company to open the account are considered before approving the account opening.
6-2 The Authority is notified directly immediately upon opening the account via a letter issued by the Reporting Officer to the Authority.
6-3 No business relationship is commenced with an exchange institution without presenting its license and proof of its registration in the register of exchange companies and offices at the Central Bank of Syria. Work for the purpose for which the relationship was established ceases immediately upon learning of the withdrawal of the institution's license and its deletion from the register, provided that the relationship is completely terminated immediately upon the completion of the institution's or company's liquidation.
6-4 No business relationship is commenced with an internal transfer company without presenting a duly certified copy of its license and the documents authorizing it to practice internal transfer activity. Work for the purpose for which the relationship was established ceases immediately upon learning of the cancellation of its license or the cancellation of the approvals authorizing it to practice the activity, provided that the relationship is completely terminated immediately upon the completion of the company's liquidation.

6-5 Opening bank accounts for internal transfer companies in currencies other than Syrian Pounds is prohibited, unless they obtain approval from the Management Committee of the Anti-Money Laundering and Counter-Terrorist Financing Authority.
6-6 Conducting any operation between accounts of owners of an exchange institution or internal transfer company or their partners or shareholders holding 5% or more of its capital or its general manager or accounts of legal persons in which they have effective influence, directly or indirectly, on one hand, and accounts of the related exchange institutions and internal transfer companies opened at the bank on the other hand, is prohibited.
6-7 Accounts of exchange institutions and internal transfer companies are used only to conduct operations these institutions and companies are authorized to conduct duly, including operations related to managing their business, such as paying their expenses, employee salaries, and distributing their profits. The branch must immediately notify the Verification Unit of every case discovered, as well as any attempt to conduct the operation, and the Authority is notified of every violation discovered.
6-8 Accounts of exchange institutions and internal transfer companies, and accounts of their owners, partners, shareholders, managers, authorized signatories, their spouses, ancestors, descendants, or employees therein are considered high-risk accounts and are subject to the enhanced due diligence measures stipulated in this guide.
6-9 Executing any operation for the benefit of an exchange company or internal transfer company through bank accounts not opened in its name is prohibited, including accounts of its owners, partners, shareholders, managers, authorized signatories, their spouses, ancestors, descendants, or employees therein.

7. All operations of the bank accounts belonging to owners of exchange institutions and internal transfer companies or their companies, shareholders, managers, authorized signatories, their spouses, ancestors, descendants, or employees therein, opened at the bank or in other banks, are documented in a way that allows ensuring that these operations are not related to the exchange institution or internal transfer company conducting its operations through these persons' accounts.
7-1 A report is filed with the Authority if the company executes any operation through any of the accounts not opened in its name as described above, as well as any attempt to execute the operation.
7-2 The Authority is notified of any accounts where suspicions exist that they are used for unlicensed exchange or transfer operations. It is also notified of any credits to accounts by other persons where suspicions exist that they result from illicit exchange or transfer activities.
7-3 The mentioned companies are not granted any chequebooks that are endorsable, and all cheques include the phrase "Pay to the first beneficiary only".
7-4 When cashing any cheque drawn on the bank from any exchange institution or internal transfer company, and if the cheque value equals or exceeds ten thousand (10,000) US dollars or its equivalent in other foreign currencies, or one hundred million SYP in case of cheques denominated in Syrian Pounds, a statement from the institution or company is required containing information about the cheque and the economic justification for the operation, in addition to information indicating whether this cheque or operation is against

the institution or company receiving cash, and the source of these funds, their destination, and the identity of the beneficiary and beneficial owner.
7-5 When executing any transfer based on a request from an exchange institution or internal transfer company for the benefit of one of its customers, a statement from the institution or company is required containing information about the operation, particularly information related to the source of the sender's funds, country of sending, sender's address, sending and corresponding company, the transfer's unique identifier and date of receipt, and the economic justification, in addition to information indicating whether this cheque or operation is against the institution or company receiving cash.
7-6 When any exchange company or internal transfer company makes cash deposits from its customers' accounts, or when such deposits are accepted from the mentioned companies' customers into these companies' accounts, the deposit operation and its justifications and parties must be documented. The branch must notify the Verification Unit of any attempt to deposit by these institutions and companies into their customers' accounts that is concealed by attributing them to natural persons, which in turn notifies the Authority according to regulations.
7-7 The monetary thresholds specified above are subject to amendments issued by decisions of the Anti-Money Laundering and Counter-Terrorist Financing Authority and are reflected in the control procedures applied in the Verification Unit.

Record Preparation and Retention:
The IT Management ensures securing all requirements for implementing the anti-money laundering program in terms of working to secure the required software and reports that assist the Verification Unit in the ongoing monitoring of operations.
Likewise, Cham Bank is committed to retaining documents related to operations and business relationships and all records and other documents through secure storage and electronic archiving according to the following principles:

- Records and documents related to all local and international operations for a period of 10 years after the completion of the operation, regardless of whether the account or business relationship is ongoing or has been terminated.
- Records and documents related to established permanent business relationships with customers, especially copies of identification documents and correspondence related to activity, for a period of 10 years from the date of termination of the business relationship.
- Records and documents related to occasional business relationships or transactions, especially copies of identification documents, for a period of 10 years from the date the transaction was conducted.
- Results of any analyses conducted (e.g., analyses related to determining the background and purpose of large, complex, unusual operations) for at least 5 years after the termination of the business relationship.
- Records and documents related to unusual or suspicious operations for a period of 10 years from the date they were conducted. In case of judicial intervention, retention is for 10 years after the issuance of the judicial ruling.

- Records and documents related to internal and external audits specific to the anti-money laundering and counter-terrorist financing program at the bank for a period of 10 years from the date of this audit.
- Records and documents related to training on anti-money laundering and counter-terrorist financing for a period of five years.
- Storage is done in a way that ensures easy and prompt retrieval of documents and records upon request, whether from inside the bank or by an external party, especially the Authority, within a period not exceeding three working days after the request.

Ongoing Monitoring and Detection of Suspicious Transactions:
1 Monitoring Cash Operations
1-1 Procedures for Monitoring Cash Operations in Branches
All branches are committed to all administrative instructions regulating cash deposits and withdrawals and the provisions of Decision /19/ and this guide. Likewise, all employees are committed to reporting any suspicious operation or attempt to conduct a money laundering or terrorist financing operation according to what is stipulated in this guide.
1-1-1. Inquiring from the customer about the source of their funds and their destination for cash operations whose value reaches or exceeds one hundred million Syrian pounds or its equivalent in foreign currencies, whether a single operation or several interconnected operations.
1-1-2. The inquiry about the source of funds and their destination is done by filling out the required data shown on the withdrawal or deposit slip.
1-1-3. The employee executing the operation is committed to filling all fields in the operation window on the banking system for operations that reach or exceed one hundred million Syrian pounds and under the conditions mentioned above.
1-1-4. Taking the customer's signature on the beneficial owner form for operations they execute on their account on behalf of others, and requesting from the customer documents proving the relationship with the beneficial owner in addition to a copy of the ID document.
1-1-5. All employees are committed not to execute any operation for the customer outside the account they hold with us, except in cases where the customer is not a direct party in the operation or in operations that do not exceed one million Syrian pounds.
The bank may exempt some of its customers from declaring the source of funds and their destination provided that:

1. The customer's relationship with it has lasted more than a year.
2. The decision is made after conducting a study of the customer's activity, account movement, pace, and reputation, so that there are serious justifications for granting this exemption in light of the studied information.
3. The exemption decision is issued by the Compliance Verification Unit.
4. This decision includes setting a new maximum limit according to the customer's circumstances, upon exceeding which declaration of the source of funds or their destination is required.

The duration of such a decision is limited to one year, and for renewal, the customer's activity, account movement, pace, and reputation are re-studied.

1-2 Procedures for Monitoring Cash Operations in the Verification Unit

1-2-1. The Verification Unit follows up on operations through special reports printed within the unit showing the cash operations that took place the previous day and conducts appropriate analyses and reconciliations.

1-2-2. The Unit exercises the authority to communicate directly with branch managements for clarification on any operation and request documents it deems appropriate to reach conviction about the integrity of the operation. The right to request additional documents is restricted to the Reporting Officer or his deputy.

1-2-3. The Verification Unit, represented by the Reporting Officer or his deputy, may request the suspension of a specific operation or a specific type of operations for the customer or account until certain documents are presented.

1-2-4. When executing cash deposit and withdrawal operations, or several interconnected deposit or withdrawal operations, whose value equals or exceeds two hundred and fifty million Syrian pounds or its equivalent, they must be reviewed and examined by the Reporting Officer after execution.

1-2-5. The Operations Monitoring Officer in the branch monitors cash operations conducted on customer accounts that reach or exceed one hundred million Syrian pounds or its equivalent in foreign currencies, according to what is stated in the approved procedures manual for operations monitoring of the Verification Unit.

1-2-6. If the monitor suspects any operation that may conceal an attempt to launder money or finance terrorism, due diligence is conducted by inquiring with the branches about the operations and knowing the source of the customer's funds and their destination.

1-2-7. A report is raised to the Reporting Officer informing him of any suspicious operations and the extent of the branches' adherence to the required directives.

1-2-8. The monetary thresholds specified above are subject to amendments issued by decisions of the Anti-Money Laundering and Counter-Terrorist Financing Authority and are reflected in the control procedures applied in the Verification Unit.

2. Incoming and Outgoing Transfers

Firstly: The Bank as the Originator

1- The provisions of control apply to all financial transfers if their value exceeds five hundred thousand Syrian pounds or its equivalent, whether conducted within Syrian territories or between Syrian territories and abroad, and whether within the framework of permanent business relationships or within the framework of occasional business relationships or transactions. The specified amount threshold is subject to amendments issued by the Anti-Money Laundering and Counter-Terrorist Financing Authority.)
2- The control provisions are not applied when the transfer relates to an operation conducted with a credit card or any card issued by a bank, as long as the card number accompanies the set of transfers resulting from the operation, except when using this card as a means of payment to execute a transfer from one person to another.
3- The control provisions are not applied when executing financial transfers between banks and their own accounts within the framework of financial settlements between them.

1. Monitoring Outgoing and Incoming Transfers in Branches

It is ensured that all data related to the beneficiary of outgoing transfers are complete as follows:

1. Name of the ordering customer and their account number.
2. Address of the ordering customer.
3. Name of the beneficiary and their account number.
4. Purpose of the transfer or its economic justification if its value exceeds five hundred thousand Syrian pounds or its equivalent for incoming transfers.

When the beneficiary does not hold an account with our party, that transfer cannot be executed without following the identification and verification procedures stipulated in the administrative instructions for account opening documents.

2. Monitoring Outgoing and Incoming Transfers in the Verification Unit:

- The Verification Unit, within the framework of ongoing monitoring of banking operations, ensures that all outgoing and incoming transfers meet all the conditions mentioned in Decision No. 19/ and that all executed transfers are based on a clear economic justification, and also ensures that branches or the operations department do not execute transfers, whether outgoing or incoming, without the full required data.
- It ensures that the customer's economic activity and business volume are consistent with the economic justification of transfers sent and received to their account through special reports on transfers printed periodically.
- It provides the Anti-Money Laundering and Counter-Terrorist Financing Authority with a monthly report on outgoing and incoming transfers according to the Authority's instructions.

Secondly: The Bank as an Intermediary:

1. If the bank participates as an intermediary in executing the transfer without being the originator or recipient, it must ensure that all information attached to the transfer related to the ordering customer and the beneficiary remains accompanying it during the transfer.
2. If the bank is unable to keep the aforementioned information attached to the transfer for technical reasons, it must retain all attached information as received for five years, enabling it to provide the available information to the receiving financial and banking institution within three days of the request.
3. Cham Bank has the right to refuse to execute the transfer or suspend its execution in case of non-availability of all requirements stipulated in Decision No. 19 regarding the parties and the economic justification for the transfer and the address of both the sender and the beneficiary, depending on the degree of risk estimated by management.

Thirdly: The Bank as Beneficiary

1. When receiving transfers, it is ensured that obtaining the required information related to the source of the transfer and its beneficiary is completed, and transfers missing the required information about the ordering customer and the beneficiary are identified to

take the appropriate action, whether returning the transfer, requesting clarifications, or completing missing data from the originating bank of the transfer.

2. Data related to the beneficiary is verified, based on the documents specified in Article 31 of Decision No. /19/ (instructions for requesting approved identification documents existing within branch work procedures) and this information is retained according to what is stated in Article 37 of Decision No. /19/ mentioned above in IT Management and Electronic Archiving Management.

3. Monitoring Transfers Between Customers

The employee, when executing a transfer request, ensures that the economic activity of the customers is consistent with the transfer's justification and has the right to request documents confirming the validity of this justification if the relationship between the transferor and the beneficiary is unclear.

Taking into account the administrative instructions and branch work procedures in this regard, and without prejudice to the branch's obligation to report any suspicious operation according to the procedure stipulated in this guide for internal reporting.

The Verification Unit, in light of its duties in ongoing monitoring of operations conducted by customers, prints special reports showing all transfers between customer accounts at the bank and the rationality and consistency of their justifications with their economic activity, business volume, and usual account movement. The employees of the Verification Unit and operations monitors have the right within this task to request any clarifications or documents from the concerned branch (and the right to request any additional documents related to the operation is restricted to the Reporting Officer or his deputy). This is according to the approved procedures for monitoring operations in the Verification Unit.

4. New Accounts

4-1 Monitoring the Opening of New Accounts in Branches

The branch must fully adhere to the administrative instructions for account opening documents. These instructions are the minimum that must be followed for customer identification and verification. It is the branch's duty to request additional information and documents if it finds the information insufficient or suspects that some of it is incorrect, considering raising a report to the Verification Unit.

4-2 Monitoring the Opening of New Accounts in the Verification Unit:

- The Operations Monitor in the branch pulls a special report on new accounts opened the previous day.
- Monitoring accounts created daily and verifying the completion of data for new accounts in compliance with Decision 19.
- Communicating with branches to complete or modify data for new accounts to comply with Decision 19.
- Raising the report to the Reporting Officer and informing him of the extent of the branches' adherence to the required directives.

Matching the names of new account holders daily with local and international blacklists and preventive freeze lists included in the national preventive freeze system.

For this purpose, he has the right to send observations he finds to the concerned branch and request any document in the branch's possession, as well as request the branch to complete or modify any missing or unclear data.

5. Power of Attorney Register

Each branch of the bank maintains a special register for powers of attorney containing all powers of attorney organized in the branch on customer accounts according to the following:

5-1 Date of the power of attorney - Full personal data of the agent - The agent's file number on the banking system - Economic activity of the agent - Name of the principal - Account number of the principal - Economic activity of the principal - Type of power of attorney - Power of attorney number - Relationship between the principal and the agent - Expiry date of the power of attorney.

5-2 The agent is considered a permanent customer, and thus must be identified and verified according to the procedures followed for identifying permanent customers, and a file is opened for them on the banking system.

5-3 The nature of the relationship between the principal and the agent must be understood, and it must be ensured that the beneficial owner of the account and the transactions executed on it is the principal and not the agent himself.

5-4 An internal report must be organized to the Reporting Officer if there is any suspicion that the true beneficiary of the account is the agent himself and not the principal account holder, according to the reporting procedure stipulated in this guide.

5-5 It is the responsibility of the Operations Monitor in the branch to periodically verify the power of attorney register and the integrity of the data and ensure that all powers of attorney organized in the branch have been included in the register by matching the paper copies with the register maintained in the branch.

6. Cheques

6-1 Monitoring Cheques in Branches:

6-1-1 Branches are prohibited from issuing any bank cheques against cash for persons who do not hold an account with our party.

6-1-2 Likewise, they are committed not to issue any bank cheques for our customers against cash without depositing those funds into their accounts first and verifying the source of those funds.

6-1-3 Re-identifying and verifying the customer requesting a chequebook for the first time.

6-1-4 Not granting any chequebook to customers who are proven to misuse cheques by using them as a guarantee instrument and not a payment instrument.

6-1-5 Taking enhanced due diligence measures when cashing or depositing cheques endorsed in favor of a third party, in a way that shows the relationship between the first beneficiary and this third party.

6-1-6 Taking enhanced due diligence measures as stipulated in this guide when the customer deposits a cheque drawn on an external banking and financial institution, or in the case of traveler's cheques.

6-2 Monitoring Cheques in the Verification Unit

6-2-1. The Operations Monitor in the branches monitors cheques conducted on customer accounts that reach or exceed one hundred million Syrian pounds or its equivalent in foreign currencies.

6-2-2 Verifying the issuing party of the cheque and the beneficiary party and the relationship between them, and verifying that the cheque does not conceal money laundering and terrorist financing operations or any illegal operation according to the approved procedure for monitoring operations (Verification Unit procedures).

6-2-3 A copy of the report is raised daily to the Reporting Officer or his deputy, and a report is duly organized regarding any suspicious operations and the extent of the branches' adherence to the required directives.

6-2-4 The monetary thresholds specified above are subject to amendments issued by decisions of the Anti-Money Laundering and Counter-Terrorist Financing Authority and are reflected in the control procedures applied in the Verification Unit.

7. Monitoring Operations Conducted Through Modern Technological Means

No electronic service can be issued and offered to customers before coordinating with the Verification Unit to establish controls and procedures that facilitate the process of monitoring those services, ensuring the following:

7-1 Pre-paid card services.

7-1-1 Setting appropriate limits for means of loading these cards and their uses, consistent with the purposes for which they were issued...

7-1-2 Setting appropriate limits for the value of each card, and the number of cards that can be issued per customer, consistent with the purpose of issuance and the risks associated with this customer.

7-1-3 Ongoing monitoring of the movement of transactions with those cards and extracting exceptional reports for any unusual operations conducted using them.

7-1-4 Enabling the suspension of use of cards misused by customers, including this condition within the contract terms with customers.

7-1-5 Taking into account full compliance with governing laws and instructions of the Central Bank of Syria related to pre-paid cards.

7-2 Banking and financial services using mobile phones:

7-2-1 Adequately considering the requirements related to transfers when using mobile phones to provide banking services.

7-2-2 The possibility of benefiting from banking and financial services via mobile phone is suspended when the customer misuses this service, and this condition is included within the contract terms with customers.

7-2-3 Ongoing monitoring of operations, and extracting exceptional reports for any unusual operations conducted using this channel.

7-2-4 Setting reasonable limits for loading accounts that benefit from this channel, as well as for the value of operations that can be executed through that service.

7-2-5 Taking into account full compliance with governing laws and relevant instructions of the Central Bank of Syria.

Internal and External Reporting Requirements:

Policy and Requirements for Reporting Suspicious Transactions.

1. The Reporting Officer is committed to reporting to the head of the Authority or his delegate details of operations suspected of concealing money laundering or terrorist financing, as well as attempts to conduct these operations, or funds suspected to be proceeds of one of the crimes listed in paragraph (c) of Article One of Legislative Decree No. /33/ and its amendments, or funds related to terrorism or used by terrorists or terrorist organizations or those who finance terrorism. No operation is considered suspicious and requires reporting except after considering the following matters before considering it suspicious:

1-1. If the operation does not involve an apparent or obvious economic or legitimate purpose.

1-2. If the size or pattern of the operation falls outside the customer's risk characterization or outside the framework of information possessed by the bank.

1-3. If the size or pattern of the operation falls outside the framework of any previous pattern of the customers' own transactions or the size or pattern of these transactions.

1-4. The customer's refusal to give a full explanation of the operation or provide complete information about it.

1-5. If the operation involves the use of accounts, companies, or external relationships not justified by the customer's economic need.
1-6. If the transaction involves the unnecessary passage of funds through a third party other than the account holder.
1-7. Any other matters related to the transaction that the bank deems necessary to consider.

2. Internal Reporting Requirements:
2-1. It is the responsibility of all employees of Cham Bank to report any suspicious operation that may conceal money laundering or terrorist financing based on the standards and indicators that may indicate the existence of such operations, immediately upon their occurrence or knowledge thereof, and by the next working day at the latest.
2-2. Reporting is done by the employee directly to the Reporting Officer via internal email and in a manner that ensures the confidentiality of the report.
2-3. The report must contain a full explanation of the operation subject to the report with all documents in the employee's possession regarding the operation.
2-4. The employee is required to report when there are logical reasons to suspect the operation, regardless of the amount or whether the operation involves tax matters, and even if the business relationship with the customer has been terminated.
2-5. The concerned employee receives a written acknowledgment of receipt from the Reporting Officer confirming receipt of the report. This notice includes a reminder to the employee not to disclose any information and not to take any action that might alert the customer.
2-6. The Reporting Officer ensures the confidentiality of the report and documents it appropriately.
2-7. The employee commits to continuing to automatically provide the Reporting Officer with details of all subsequent operations conducted by the customer unless the Reporting Officer requests him to stop.
2-8. The Reporting Officer is committed to studying the case based on the available data at the bank and has the right to request any additional information from any party within the bank to then decide whether the operation is suspicious or not.
2-9. The Reporting Officer is committed to providing the concerned employee in writing with the result of the decision taken.

3. Requirements for Reporting to the Anti-Money Laundering and Counter-Terrorist Financing Authority
3-1. The Reporting Officer is committed to studying the case within a maximum period of one month from the date of receiving the report. He may decide to place the account and related accounts under enhanced monitoring for an additional similar period to confirm the operations and reinforce or negate the suspicion.
3-2. Reporting is done by the Reporting Officer directly to the head of the Authority or his deputy according to the approved form attached to Decision No. 19, with all details and documents related to the operation and the customer, as well as the facts and bases relied upon for the suspicion, in case conviction is formed that the case requires reporting according to the approved indicators and case data.

3-3. When necessary, refraining from executing any unusual operation on the account except after consulting the Authority.

4. Post-Reporting Phase:

4-1. Any employee is prohibited from destroying any records related to the customer or the business relationship subject to the report without referring to the Reporting Officer, who in turn consults the Authority in this regard.

4-2. Restricting any operation or closing any account for the customer subject to a report on a suspicious operation or funds cannot be done before referring to the Verification Unit, which in turn consults the Authority regarding this, so that it does not lead to alerting the customer by mistake.

4-3. It is the responsibility of the Reporting Officer to prepare and retain records related to the following:

a. Details of each internal report related to a suspicious operation or funds.

b. Details of each report on a suspicious operation submitted to the Authority.

5. Alerting the Customer by the Bank

5-1. The bank refrains from disclosing any suspicious transaction reports or specific information that has been reported to the Authority.

5-2. The bank should ensure that its employees are aware of the sensitivity of the issues surrounding alerting the customer or disclosure and its consequences.

5-3. If the bank believes or has reasonable grounds to believe that the customer may become alerted through taking due diligence measures, it must submit a report on the suspicious operation instead of taking the mentioned due diligence measures.

6. Procedures for Protecting Information Related to Suspicious Transaction Reports

6-1. The bank must take all reasonable measures to ensure the protection of information related to suspicious transaction reports, including:

6-1-1. Ensuring that information on suspicious transaction reports is not disclosed to any person without the approval and permission of the Reporting Officer, except for members of the Board of Directors and the Chief Executive Officer.

6-1-2. Not granting the Reporting Officer's approval to disclose information related to suspicious transaction reports to any person, unless he is certain that this disclosure will not result in alerting the customer.

6-1-3. When the Reporting Officer approves the disclosure of information related to suspicious transaction reports, he must prepare and retain appropriate records proving that this disclosure does not result in alerting the customer.

6-2. The bank is prohibited from providing any funds or any financial service, including transfers, or others, directly or indirectly, wholly or jointly with others, for the benefit of persons and entities listed within the lists specified in the decision of Mr. Prime Minister No. 851 dated 13/3/2014 and its amendments, as well as for the benefit of persons and entities acting on behalf of the listed persons and entities or acting under their direction, unless a license or authorization is available or unless notified otherwise.

6-3. The bank must notify the committee formed pursuant to the decision of Mr. Prime Minister No. 851 dated 13/3/2014 and its amendments, of any information related to frozen funds according to the provisions of the mentioned decision or any measures taken to implement its provisions.

6-4. The bank is committed to referring to the lists of terrorists specified in the decision of Mr. Prime Minister No. 851 dated 13/3/2014 and its amendments when conducting any operation or entering into a new relationship with any person to ensure that their name is not listed within these lists. In case of a matching or similar name, the Verification Unit must be referred to, which in turn studies the case and acts pursuant to the mentioned decision if it is proven that the name is listed within those lists, where the Authority must be notified immediately.

6-5. The bank credits any accounts frozen pursuant to the decision of Mr. Prime Minister No. 851 dated 13/3/2014 and its amendments with any amounts or transfers, provided that these amounts added to the mentioned accounts are frozen, and it must notify the committee formed pursuant to the provisions of the mentioned decision of these operations immediately.

6-6. All amounts resulting from any contracts, agreements, or obligations concluded or arising before the date of listing on the lists referred to in this article are added to the accounts frozen pursuant to the decision of Mr. Prime Minister No. 851 dated 13/3/2014 and its amendments, including profits and interest, provided that all these amounts are subject to freezing.

6-7. The bank adheres to all other provisions of the decision of Mr. Prime Minister No. 851 dated 13/3/2014 and its amendments.

Implementation of Freezes Issued by the Authority and Relevant Parties:

Cham Bank is committed to the immediate freezing of any bank balances or accounts belonging to persons whose accounts are ordered frozen by the Anti-Money Laundering and Counter-Terrorist Financing Authority or any other judicial or custodial authority, so that those accounts are not allowed to be moved except as permitted by relevant decisions and laws to settle amounts due to the bank. Likewise, amounts received into those accounts are recorded and frozen similarly to the amounts initially frozen.

The freeze is only lifted by a lift decision issued by the authority that decided to freeze those accounts.

Employee Appointment Standards

Cham Bank is committed to high standards when appointing or employing staff and officials according to the following:

a- Purposes of combating money laundering and terrorist financing

1- Employees with significant influence: They are employees who play a fundamental role in combating money laundering and terrorist financing, such as executive managers, compliance managers, internal audit managers, heads of various departments, reporting officers, and workers in compliance, internal audit, risk, and compliance verification unit directorates.

2- Other employees.

b The appointment procedures for appointing employees with significant influence ensure reassurance about their character and integrity and the knowledge, skill, and ability to act honestly, professionally, and independently. The appointment procedures for other employees ensure reassurance about their integrity.

c - The appointment process requires at a minimum the following conditions:

4- Obtaining a curriculum vitae or sufficient background about the candidate and verifying it.
5- Verifying employment history and qualifications.
6- Obtaining information or details about any criminal convictions or regulatory authority procedures if they exist and verifying them.
7- Ensuring the accuracy and completeness of information obtained for appointment purposes through appropriate procedures outlined in the appointment procedures manual of the Human Resources Management.

Continuous Training on Anti-Money Laundering and Counter-Terrorist Financing Procedures:

a. All employees of Cham Bank are subjected to continuous training courses by developing and implementing a continuous and appropriate training program to train employees and officials on anti-money laundering and counter-terrorist financing.

b. The training program is designed to ensure that employees and officials in the bank are aware of the following:

1. Legal, regulatory, and supervisory responsibilities and obligations related to anti-money laundering and counter-terrorist financing.
2. The role of employees and officials in combating money laundering and terrorist financing and in applying the approved anti-money laundering and counter-terrorist financing program in the bank, and their awareness of the responsibility upon them if they become involved in money laundering or terrorist financing and their non-compliance with the legal, regulatory, and supervisory requirements related thereto.
3. The bank's management of money laundering and terrorist financing risks and the role of the Reporting Officer, the importance of due diligence measures and ongoing monitoring, introduction to methods used in money laundering and terrorist financing, vulnerabilities of products offered and worked with by the bank, identifying suspicious operations, processes and procedures for preparing internal suspicious transaction reports, etc.

c- Training needs are determined by the Human Resources Management, taking into account existing expertise, skills, and capabilities, required functions and roles, the size of the bank's business and its risk characterization, the result of previous training, and expected needs.

d- The training program on anti-money laundering and counter-terrorist financing ensures providing continuous training to ensure that employees maintain their knowledge, skills, and capabilities in the field of anti-money laundering and counter-terrorist financing and update them to keep pace with new developments, including the latest techniques, methods, and trends related to anti-money laundering and counter-terrorist financing.

e- The training program is reviewed whenever necessary, and the result of each review of the anti-money laundering and counter-terrorist financing program is taken into consideration. Whenever the review shows gaps in anti-money laundering and counter-terrorist financing training requirements, an action plan must be prepared to address these gaps in a timely manner.

f- The training material is prepared by the Reporting Officer and the Verification Unit and is approved by the Executive Management in coordination with the Human Resources Management.

Internal and External Audit:

Internal Audit:

1- The Internal Audit Department conducts an annual review of the effectiveness of the anti-money laundering and counter-terrorist financing program, including the policies, procedures, and controls for anti-money laundering and counter-terrorist financing in the bank and the extent of compliance with them, by including this review in the annual plan of tasks of the Internal Audit Department approved by the Board of Directors.

2- The internal audit policies and procedures approved by the Board of Directors ensure the following:
   a. Auditing the effectiveness of the anti-money laundering and counter-terrorist financing program.
   b. Auditing the effectiveness of anti-money laundering and counter-terrorist financing policies, procedures, and controls in addressing the identified risks.
   c. The extent of compliance with the application of anti-money laundering and counter-terrorist financing policies, procedures, and controls.
   d. The effectiveness of ongoing monitoring of operations, including the effectiveness of alert standards for unusual operations.
   e. The effectiveness of employee training.

3- It must be continuously ensured that the Internal Audit Department possesses employees with knowledge and experience in such auditing, and that the scope and periodicity of the audit are appropriate to the identified risks, and the adequacy of resources allocated to it.

4- The internal audit body is committed to following up on discovered gaps and following up on its recommendations regarding these gaps.

External Audit:

1- The external audit body, alongside its other tasks, and within the framework of its tasks in evaluating the bank's internal procedures and controls, is tasked with ensuring compliance with legal, regulatory, and supervisory controls related to anti-money laundering and counter-terrorist financing, and presenting the results of this review in a letter to the Board of Directors.

2- The external audit body is chosen on the condition that it possesses employees with knowledge and experience in such auditing, and that the scope of the audit it conducts is appropriate to the identified risks.

VI: Relationship with the Authority:

The bank, within the framework of responding to cooperation requests received by the Authority, is committed to the following:

1. Preparing a database in the form of a list linked automatically to the information system used by the bank, containing all names and entities specified pursuant to paragraph /c/ of Article Ten of the Legislative Decree, and specified pursuant to paragraph /e/ of Article Six of the executive instructions, for use within the framework of the banking and financial institution's commitment to these requirements.
2. Exercising accuracy and necessary care while responding to such requests.

3. Confidentiality of the Authority's requests, and not informing those who are not concerned about them.
4. Informing the Authority and the competent supervisory body immediately in case any obstacle affects its ability to fulfill the legal obligations imposed on the bank under the applicable laws and regulations related to anti-money laundering and counter-terrorist financing.
5. Adopting electronic correspondence with the Authority, except in emergency and special cases approved by the Authority until that situation ceases.
6. Providing the Authority with contact data for the Reporting Officer and the Compliance Verification Unit and the names of employees therein every six months in an updated manner or when any change occurs thereto.

VII: Conclusion:

This guide was prepared by the Reporting Officer at the bank based on the requirements of Legislative Decree No. 33 of 2005 and its amendments by Legislative Decree 27 of 2011 concerning combating money laundering and terrorist financing, and Legislative Decree No. /46/ of 2013, as well as Decision No. 19 / of 2019 issued by the Management Committee of the Anti-Money Laundering and Counter-Terrorist Financing Authority and its subsequent amendments.
Taking into consideration the Forty Recommendations and their annexes issued by the Financial Action Task Force (FATF).

Translated from the attached document..

Sworn Translator