The Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Guide

AML/CTF Department
Saudi Central Bank
RABI' I 1441H (November 2019)

Table of Contents

I. Introduction

The Kingdom of Saudi Arabia is committed to detecting and preventing laundering of proceeds of ML/FT crimes as well as to punish perpetrators in accordance with the Anti-Money Laundering Law, the Law on Terrorism Crimes and Financing, and their Implementing Regulations. Saudi Arabia had previously ratified and signed agreements at the international level. It signed the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances in Vienna in 1988 and the United Nations Convention against Corruption in January 2004. It also ratified the International Convention for the Suppression of the Financing of Terrorism in New York in 1999 and the United Nations Convention against Organized Crime in Palermo in 2000. Saudi Arabia joined the Financial Action Task Force (FATF) in June 2019 to be the 1st Arab country and the 37th country in the world to obtain the membership. At the regional level, Saudi Arabia ratified the Arab Anti-Terrorism Agreement under the auspices of the Arab League at a conference held in April 1998. It also signed and ratified the Organization of Islamic Conference (OIC) Agreement for the suppression of international terrorism in July 1999 as well as the GCC Anti-Terrorism Agreement in May 2004. Saudi Arabia is a founding member of the Middle East and North Africa Financial Action Task Force (MENAFATF), which created in November 2004. Furthermore, many developments in the international financial sector have been witnessed in the recent years, including the efforts made for combating ML/TF. SAMA has adopted various initiatives that include measures and other criteria in response to international developments in this field. This includes the issuance of a guide for the implementation of Security Council Resolutions relevant to combating terrorism and its financing to ensure optimal application of updated procedures and mechanisms relating to such resolutions. SAMA also issued a guide for the implementation of Security Council Resolutions relevant to preventing proliferation of weapons of mass destruction and their financing to ensure that financial institutions optimally apply the relevant procedures and mechanisms. Due to the importance of financial institutions in detecting and preventing ML/TF transactions, SAMA has prepared this Guide to help financial institutions abide by the minimum regulatory requirements and to protect these institutions from being used as a conduit for illegal

transactions arising from ML/TF activities and other crimes. This can contribute to enhancing and maintaining confidence in the integrity and reputation of the financial system in Saudi Arabia.

Chapter II: Purpose

- The purpose of this Guide is to help financial institutions operating in Saudi Arabia and licensed by SAMA to develop and adopt a risk-based approach for conducting their business to meet the requirements of the Anti-Money Laundering Law, issued by Royal Decree No. (M/20) dated 05/02/1439H, and its Implementing Regulations, issued under the Decision of the Presidency of State Security No. (14525) dated 19/02/1439H, as well as the Law on Combating Terrorism Crimes and Financing, issued by Royal Decree No. (M/21) dated 12/02/1439H, and its Implementing Regulations, issued pursuant to the Council of Ministers' Resolution No. (228) dated 02/05/1440H.
- The requirements mentioned in this Guide reflect the obligations stated in the Anti-Money Laundering Law, the Law on Terrorism Crimes and Financing, and their Implementing Regulations. Such requirements do not impose any additional obligations on financial institutions supervised by SAMA.
- The requirements stated in this Guide are obligatory and are the minimum requirements to be complied with by financial institutions. Moreover, a financial institution should put in place additional appropriate measures as required by the results of its approved risk assessment.

Chapter III: Legal Framework

- Article (24) of the Anti-Money Laundering Law stipulates that "To carry out their mandate, supervisory authorities shall: (d) issue guidance, instructions, rules or any other instruments to financial institutions, designated non-financial businesses or professions, and non-profit organizations in pursuance of the provisions of this Law."
- Article (82) of the Implementing Regulations of the Law on Combating Terrorism Crimes and Financing stipulates that "To carry out their

mandate, supervisory authorities shall: (4) issue instructions, rules, guidance, or any other instruments to financial institutions, designated non-financial businesses or professions, and non-profit organizations in implementation of the provisions of this Law."

- Paragraph (4) of Article (1) of the Implementing Regulations of the Anti-Money Laundering Law stipulated that "The supervisory authorities as stipulated in Paragraph (12) of this Article include: (a) The Saudi Central Bank."
- Paragraph (4) of the Implementing Regulations of the Law on Combating Terrorism Crimes and their Financing stipulates that "The supervisory authorities bellow, each according to its jurisdiction, referred to in Article 1/22 of the Law shall include (4) Saudi Central Bank."
- Supreme Royal Order No. (55871) dated 09/11/1436H providing for the approval for making King Salman Humanitarian Aid and Relief Center as the sole authority to collect relief, charitable or humanitarian donations, whether from government or private sources, to deliver them to those in need outside the country.
- The Council of Ministers Resolution No. (226) dated 02/05/1440H states that SAMA is the competent authority by law to operate, monitor and supervise payment and financial settlement systems and their services in Saudi Arabia. It may issue rules, instructions and licenses in accordance with the standards applied by SAMA in this regard.

Chapter IV:Definitions

- **Anti-Money Laundering Law:** The Anti-Money Laundering Law issued by Royal Decree No. (M/20) dated 05/02/1439H.
- **Law on Combating Terrorism Crimes and Financing:** The Law on Terrorism Crimes and Financing issued by Royal Decree No. (M/21) dated 12/02/1439H.
- **Implementing Regulations of the Anti-Money Laundering Law:** The Implementing Regulations issued by the Decision of the Presidency of State Security No. (14525) dated 19/02/1439H.
- **Implementing Regulations of the Law on Combating Terrorism Crimes and Financing:** the Implementing Regulations of the Law on

Combating Terrorism Crimes Financing issued under the Council of Ministers Resolution No. (228) dated 02/05/1440H.

- **SAMA:** The Saudi Central Bank.
- **Saudi Arabia Financial Intelligence Unit (SAFIU):** A national center that receives information and reports related to crimes of money laundering, terrorist financing, predicate offenses, or proceeds of crime according to the Anti-Money Laundering Law, the Law on Combating Terrorism Crimes and Financing, and their Implementing Regulations. The SAFIU analyzes and investigates such reports and information before submitting related results to the competent authorities, promptly or upon request. The SAFIU reports to the President of State Security and has sufficient operational independence, and the President of State Security determines the organizational structure of the SAFIU.
- **Financial Action Task Force (FATF):** An inter-government organization (established in 1989 in Paris by the G7) whose tasks include setting standards and promoting effective implementation of legal, regulatory and operational measures to combat money laundering, terrorist financing, and proliferation financing as well as other threats to the integrity of the international financial system.
- **Designated Non-Financial Businesses or Professions (DNFBPs):**

This includes any of the following commercial or professional activities:

a) Real estate brokerage when entering into business relationships for buying and selling real estate of all kinds.
b) Dealing in gold, precious stones or precious metals when engaging in cash transactions with a customer equal to or over SAR 50 thousand or more, whether the transaction is carried out in a single operation or in several operations, which appear to be linked, whether through sole proprietorships or commercial companies.
c) Lawyers and anyone who provides legal or accounting services in the exercise of their professional activities when they prepare, execute or conduct transactions in relation to any of the following activities:
    i. Purchase or sale of real estate.
    ii. Management of a customer's funds, including bank accounts and other assets.

iii. Establishment, operation, or management of legal persons or legal arrangements, or the organization of related subscriptions.

iv. Sale or purchase of commercial companies.

- **Financial group:** A local group consisting of a company or any other type of legal or natural persons that exercises control and coordinating functions over the rest of the group to implement group supervision, together with branches or subsidiaries that are subject to AML/CTF policies and procedures at the group level.

a) **Financial institution:** An entity conducting, for or on behalf of a customer, one (or more) of the following financial activities or operations: Acceptance of deposits and other funds payable by the public, including private banking services[1].

b) Lending, financial leasing, or any other financing activities.

c) Money or value transfer services.

d) Issuance and management of payment instruments (such as credit cards, debit cards, prepaid cards, checks, traveler's checks, payment orders, bank transfers, and digital currency).

e) Issuance of letters of guarantee or other financial guarantees.

f) Trading in the following:

i. Checks, bills of exchange and other instruments.

ii. Currencies .

iii. Currency exchange, interest rate and financial index instruments.

iv. Negotiable securities and derivatives.

v. Commodity futures.

g) Foreign exchange transactions.

h) Participation in issuing securities and providing financial services.

i) Safekeeping and managing of cash or securities on behalf of another person.

[1] Private banking services are provided to high net worth individuals. A financial institution assigns a certain officer or a relation manager for such clients to facilitate their use of a wide range of financial services and products that usually include sophisticated operations and huge amounts. Such clients require a high level of confidentiality and thus private services are more vulnerable to ML/FT activities or proliferation.

j) Concluding protection and/or savings insurance contracts and other types of investment-related insurance as a provider, an agent or a broker of the insurance contract or any other insurance products stipulated in the Law on Supervision of Cooperative Insurance Companies and its Implementing Regulations.
k) Investment, management or operation of funds on behalf of another person.

- **Shell bank:** A bank or a financial institution that is incorporated or licensed in a country where it has no physical presence and that is unaffiliated with a financial group subject to regulation and supervision.
- **Senior management:** It includes the managing director, the chief executive officer, the general manager, their designates, the chief financial officer, and directors of key departments in charge of functions of risk management, internal audit, compliance, AML/CFT in a financial institution as well as those equivalent and any other positions specified by SAMA.
- **Senior management position:** It includes the managing director, the chief executive officer, the general manager, their deputies, the chief operating officer, the chief financial officer, or the chief actuarial officer.
- **Financial institution staff:** Members of the board of directors and its committees, executives, employees (permanent and contracted), advisors and staff of a third party.
- **Customer:** Any person who conducts, or intends to conduct, any of the following activities with the financial institution:
  a) Arranging or undertaking a transaction, establishing a business relationship, or opening an account.
  b) Signing a transaction, business relationship or account.
  c) Assigning an account according to a transaction.
  d) Transferring an account, rights or obligations according to a transaction.
  e) Obtaining permission to conduct a transaction or to control a business relationship or an account.
- **Occasional customer:** A person who does not have an existing business relationship with the financial institution but wishes to conduct a transaction through it.

- **Business relationship:** A relationship of a continuing or temporary nature that is established between a financial institution and its customers related to the activities and services provided to them.
- **Beneficiary:** A natural or legal person that benefits from a business relationship with a financial institution.
- **Beneficial owner:** A natural person who ultimately owns or exercises direct or indirect control over a customer or a natural person on whose behalf a transaction is conducted, including over a financial institution or any other legal person.
- **Person acting on behalf of a customer:** A person legally authorized to carry out or initiate any of the activities that a customer may conduct, such as an authorized person or a legal attorney.
- **Politically Exposed Persons (PEPs):** Individuals who are entrusted with prominent public functions domestically or in a foreign country or who occupy senior management positions or positions in an international organization, including the following:
    a) Heads of states or governments, senior politicians, senior government, judicial or military officials, senior executives of state-owned companies, and high-ranking officials of political parties.
    b) Directors and deputy directors of international organizations, chairmen and members of the board of directors, and similar positions.
- **Family member of a PEP:** Any natural person related to a PEP by virtue of blood or marriage until the second degree of kinship.
- **Person close to a PEP:** Any natural person who is involved with a PEP by having a real partnership in a legal entity or a legal arrangement, who has a close business relationship with such PEP, or who is a beneficial owner of a legal entity or a legal arrangement ultimately owned or controlled by such PEP.
- **Preventive measures:** All measures, procedures and controls adopted by a financial institution to mitigate the risks of ML/TF and proliferation.
- **Due diligence measures:** The process of obtaining or verifying information of a customer or a beneficial owner to enable the financial institution to assess the extent to which the customer exposes it to risks.

- **Simplified measures:** The application of preventive measures in a streamlined and simplified manner consistent with ML/TF risks posed by a customer, beneficial owner or business relationship. This includes taking simplified due diligence measures to identify and verify a customer, apply a simplified method of monitoring, and take any other simplified measures specified by the financial institution in its policy and procedures.
- **Enhanced measures:** Additional measures are taken by a financial institution when the risks of ML/TF become high. These include enhanced due diligence measures to identify and verify a real customer or beneficial owner, additional control measures, and any other measures or procedures that the financial institution specifies in its policy.
- **Transaction:** It includes all actions involving funds, properties or proceeds in cash or in kind. Examples of such actions include: Depositing, withdrawing, transferring, selling, purchasing, lending, swapping, extending of credit, mortgaging, gifting, financing and exchanging of funds in any currency, whether in cash or checks, payment orders, stocks, bonds, or any other financial instruments in addition to the use of safe deposit boxes or any other disposition of funds.
- **Funds:** These are assets, economic resources and property of any value, type or ownership, whether material or immaterial, tangible or intangible, movable or immovable, as well as documents, deeds, instruments, transfers and letters of credit in any form, whether inside or outside Saudi Arabia. They also include electronic or digital systems, bank credits that indicate ownership or interest, and all types of commercial papers, securities, and any other interests, profits or incomes resulting from these funds.
- **Monitoring process:** Follow-up of all transactions performed by customers of financial institutions, occasional customers, or the financial institution staff, with the aim of detecting any abnormal transactions.
- **Suspicious transaction:** A transaction for which a financial institution has reasonable grounds to suspect its association with money laundering, terrorism financing, a predicate offense, or proceeds of a crime, including the attempt to conduct such transaction.

- **Records:** Paper and electronic documents and reports related to transactions, business relationships, and commercial and monetary deals, whether local or external, including documents obtained under standard/enhanced/simplified due diligence measures and any documents that contribute to the interpretation of financial, commercial and cash transactions.
- **National address:** The general place of residence of a natural or legal person unless such person chooses a specific address for receiving notifications. Each address (general or specific) prepared by the Saudi Post, as the case may be, is considered an approved address subject to all legal consequences.
- **Reliable source:** The originating source of information or data on which a financial institution relies to identify a customer.
- **Third party:** The entity on which a financial institution relies on implement the due diligence measures, provided that such entity is another financial institution or an owner of a DNFBP.
- **Correspondence relationship:** It is a relationship between a correspondent financial institution and a respondent institution through an account or any other related services, such as cash management, international money transfers, check clearing, foreign exchange services, trade finance, liquidity management, and short-term lending. This includes correspondent relationships established for securities transactions or money transfers.
- **Correspondence payment accounts:** These are demand deposit accounts opened by a foreign financial institution with a local financial institution to credit deposits and checks of its customers to those accounts. Foreign customers have the power to sign their account's transactions, which enables them to carry out normal business activities at the international level. Financial institutions are prohibited from accepting this type of accounts.
- **Wire transfer:** A financial transaction carried out by a financial institution on behalf of a wire transfer originator to make an amount of funds available to a beneficiary in another financial institution, regardless of whether the originator and the beneficiary are the same person.

Chapter V: Concept of Money Laundering:

A money laundering offence shall be deemed a separate offence from the predicate offense. A conviction for the predicate offense shall not be necessary for a conviction for money laundering or to establish that funds are proceeds of crime, whether the predicate offense was committed inside or outside Saudi Arabia. The intent, knowledge, or purpose of committing the money laundering offence shall be inferred from objective factual circumstances of the case. Anyone who commits any of the following acts shall be considered to have committed a money laundering offence:

1. Transfer, transportation, or performing of any transaction with funds while knowing that they are proceeds of crime in order to conceal or disguise the illegitimate origin of those funds or to assist a person involved in the predicate offense that generated those funds to evade the consequences of committing such crime.
2. Acquiring, possession or use of funds with the knowledge that they are proceeds of crime or from an illegal source.
3. Concealment or disguise of the nature, source, movement, ownership, place, manner of disposition of, or rights associated with funds that the person knows are proceeds of crime.
4. The attempt to commit any of the acts stated in Paragraphs (1, 2 and 3) above or participation in those acts by means of agreement, assistance, incitement, counseling, advice, facilitation, collusion, plotting, or concealment.

A legal person shall be considered to have committed a money laundering offence if any of the acts mentioned above was committed in its name or for its account. Criminal liability of a legal person shall not exclude the criminal liability of its chairpersons, members of its boards of directors, its owners, employees, authorized representatives, auditors, or any other natural person who acts in its name or for its account.

There are usually three stages of money laundering, explained as follows:

1. **Depositing or Placement:** In this stage, illegally obtained funds are introduced into the financial system, with the aim of depositing cash resulting from illegal activities into the financial system in a manner

that does not attract attention. This is usually achieved through financial institutions when a customer or a person acting on their behalf engages in any of the financial activities and transactions, including acceptance of cash deposits, currency exchange, purchase of shares, and conclusion of finance contracts or protection and/or savings insurance contracts, without taking sufficient preventive measures by the financial institution to protect itself from money laundering risks.

2. **Layering:** It is the stage in which funds are transferred and moved with the purpose of concealing their origin. The aim is to disguise the illegal source of the funds introduced into the financial system. This stage may involve sending wire transfers to other financial institutions, purchase and sale of investments and financial instruments, cancellation of finance contracts or protection and/or savings insurance policies during the free look period[2], fraudulent investments, or business schemes.
3. **Integration:** In this stage, funds are brought into the economy again so that it becomes difficult to distinguish them from funds of legitimate origin. The aim is to legitimize illegal funds and integrate them into the domestic or global economy, through the purchase of financial assets, shares, or luxury goods or the investment in real estate.

Chapter VI: Concept of Terrorism Financing

Terrorist crime is any criminal act committed, individually or collectively, directly or indirectly, by a perpetrator, with the intention to disturb public order, destabilize the national security or state stability, endanger national unity, suspend the Basic Law of Governance or some of its provisions, cause damage to state facilities or its natural or economic resources, attempt to coerce any of its authorities into a particular action or inaction, harm or cause death to any person, when the purpose -by its nature or context- is to terrorize people or coerce any government or international organization into a particular action or inaction, or threaten to carry out

[2] The period of time during which a beneficiary can review the insurance policy and assess its suitability as the policyholder has the option to cancel the insurance policy (Article 26 of the Insurance Market Code of Conduct Regulations).

acts that would lead to any of the aforementioned objectives or purposes or instigate such acts. It also includes acts constituting a crime according to Saudi Arabia's obligations to any international conventions or protocols pertaining to terrorism or its financing and to which Saudi Arabia is a party, and acts included in the Annex of the International Convention for the Suppression of the Financing of Terrorism. The crime of terrorism financing is achieved through provision of funds for the commission of a terrorist crime or for the benefit of a terrorist entity or person, including the financing of a terrorist's travel and training.

Transactions related to terrorism financing are distinguished from those related to money laundering as follows:

1. Small transactions, including bank transfers and currency exchange, can be used to finance terrorist activities.
2. Terrorists can be financed using funds obtained legitimately, making it difficult for the financial institution to determine the stage in which legitimate funds become funds used to finance terrorist operations. Terrorists can derive their financing from legal and/or illegal sources.

Therefore, financial institutions shall ensure that their internal control and monitoring systems do not focus only on high-value transactions. They shall add indicators into these control systems relating to terrorism financing and the search for transactions without a clear economic purpose. In addition, financial institutions shall implement effective controls and procedures for customer identification and verification as well as continuous transaction monitoring and reporting of suspicious transactions to ensure that Saudi Arabia's financial system is not misused to finance terrorists, terrorist organizations, or terrorist acts.

Chapter VII: Governance and Responsibilities of Financial Institution

The financial institution is responsible for the effective implementation of the AML/CTF requirements and adoption of a risk-based approach to mitigate the money laundering and terrorism financing risks it faces. The

financial institution shall not consider combating money laundering and terrorism financing in isolation from other regulations and needs in the financial institution, but as part of its comprehensive risk management strategies. Therefore, the board of directors and senior management in the financial institution shall ensure that the policies, procedures and controls in place related to AML/CTF are based on the results of money laundering and terrorism financing risks. To ensure the effectiveness of the AML/CTF strategy at the level of the financial institution, the risk management process shall be reviewed continuously and updated periodically, and appropriate mechanisms, policies and procedures shall be developed to mitigate risks. The financial Institution must ensure that its employees are sufficiently aware of all the policy requirements, procedures and internal controls and are working to implement them.

Section 1: Board of Directors

The board of directors of the financial institution is generally responsible for ensuring compliance with AML/CTF requirements. In this regard, the oversight exercised by the board concerning combating ML/TF shall be in line with international best practices, including SAMA Governance Guidelines. The board shall also ensure that there is documentation relevant to its oversight function, such as minutes of meetings of the board (or board committees). The main responsibilities of the board include, but are not limited to, the following:

a) Ensuring that the ML/TF risk assessment in the financial institution is conducted accurately and covers all risks facing the financial institution in order to develop appropriate policies to manage such risks.
b) Adopting an internal policy to mitigate ML/TF risks and ensure its effective implementation.
c) Providing sufficient budget and resources, including adequate and qualified employees as well as appropriate systems and tools in order to ensure that the application of internal policies, procedures and controls is effective and consistent with the ML/TF risks identified.
d) Following up on the implementation of the ongoing and annual training programs in the field of AML/CTF for all employees as well as members of the board of directors and senior management.

e) Ensuring that appropriate independent audit mechanisms are in place so that the board can monitor the ongoing effectiveness of internal controls.

Ensuring that the appropriate actions are promptly taken and that violations are not committed when a branch or subsidiary in a country or region is unable to implement the AML/CTF requirements as stated in the Anti-Money Laundering Law, the Law on Combating Terrorism Crimes and Financing, and their Implementing Regulations due to the weakness of laws, regulations, or other domestic measures in that country or the inability to implement the appropriate measures.

f) Ensuring the receipt of regular comprehensive reports on ML/TF risks facing the financial group or financial institution, including but not limited to:

- Corrective action plans, if any, to process the results of independent audits (whether internal or external), observations of the AML/CTF compliance department and inspection reports from SAMA regarding the evaluation of the financial institution's compliance with AML/CTF requirements.
- Developments and updates in the laws and regulations for combating money laundering and terrorism financing as well as their implications on the financial institution, if any.
- Details of high ML/TF risks and potential effects on the financial institution.
- Details on the implementation of financial sanction procedures related to the UN Security Council resolutions regarding those on terrorist lists, combating proliferation, or the decisions communicated by SAMA.

Section 2: Senior Management

The senior management is responsible for the continuous implementation and monitoring of compliance with the AML/CTF requirements in the financial institution. The main responsibilities of the senior management include, but are not limited to, the following:

a) Identifying, assessing, and understanding ML/TF risks arising from new products or services, distribution channels, or customers.
b) Establishing a program for AML/CTF that includes setting up and developing policies, procedures, and controls in line with the latest means, techniques and methods of ML/TF.
c) Adopting internal procedures and controls to mitigate ML/TF risks.
d) Reviewing policies and procedures periodically (at least once a year) by establishing an appropriate mechanism for periodic review of the main AML/CTF policies and procedures to ensure that they are continuously effective and consistent with the changes in products and services of the financial institution and to address new and emerging risks from ML/TF activities.
e) Taking actions with regard to all important recommendations issued by the AML/CTF compliance department, the independent auditor, and supervisory authorities concerning the level of compliance with AML/CTF requirements.
f) Providing the board of directors with sufficient relevant information in a timely manner about matters relating to AML/CTF.
g) Providing appropriate specialized training for employees in the AML/CTF compliance department and those working in the same field on an annual basis to ensure effective performance of their duties and functions.
h) Creating a continuous training program for employees of the financial institution to enable them to obtain sufficient knowledge and understanding and fulfill their responsibilities related to AML/CTF.
i) Supporting the functions of AML/CTF compliance and independent audit appropriately in terms of staff, technical systems, information, and budget in order to effectively implement, manage and monitor the AML/CTF program requirements.

j) Following up on the implementation of the instructions and circulars issued by SAMA regarding AML/CTF.

Section 3: Financial Institution Staff

Employees of the financial institution are responsible for the implementation of policies, procedures, and controls of AML/CTF, including:

a) Following and implementing policies and procedures of AML/CTF and being aware of the need to comply with the laws, regulations, and guidelines applicable in this field.
b) Ensuring that no actions are taken on behalf of a customer when such actions are required to be taken by that customer in accordance with the internal instructions.
c) Performing daily tasks in accordance with the internal work procedures of the financial institution and in a manner consistent with the relevant laws and instructions.
d) Reporting immediately to the AML/CTF compliance officer when there are reasonable grounds for suspicion of a ML/TF transaction.
e) Refraining from disclosing or implying any information about suspicious transactions linked to a certain customer or that certain transactions are under investigation internally or externally.
f) Taking the appropriate measures to ensure that no clues are given when requesting information from a customer.
g) Providing full assistance in investigations related to ML/TF.

Chapter VIII: General Framework

The principles in this Guide have been developed in accordance with the regulatory requirements provided for in the Anti-Money Laundering Law, the Law on Combating Terrorism Crimes and Financing, and their Implementing Regulations, which aim to establish effective requirements, guidelines, and procedures to prevent the use of Saudi Arabia's financial

system for purposes of ML/TF. These principles fall under the following headings:

- ML/TF Risk Assessment.
- Internal Policies, Procedures and Controls to Mitigate Risks.
- Due Diligence Measures.
- Enhanced Due Diligence Measures.
- Simplified Due Diligence Measures.
- Record Keeping.
- Monitoring of Transactions and Activities.
- Reporting of Suspicious Transactions.
- Arrangements of AML/CTF Compliance Function.
- Independent Audit Function.
- AML/CTF Training.
- Recruitment and Follow-up Criteria.
- Correspondent Relationship.
- Wire Transfer.

Based on the above requirements, a financial institution shall prepare and adopt a risk-based approach commensurate with the nature and size of its business. Such approach shall be prepared according to the following steps:

- First Step: Identifying the inherent risks of business and business relationships as well as any other risks.
- Second Step: Determining the financial institution's risk appetite.
- Third Step: Developing preventive measures to mitigate risks based on the results of risk assessment.
- Fourth Step: Reviewing residual risks after developing the preventive measures.

- Fifth Step: Implementing the preventive measures to mitigate risks.
- Sixth Step: Reviewing and updating the risk-based approach.

Risks to which a financial institution is exposed are variable and changing over time as new products, business practices, or means of providing services, products, or transactions are developed. Therefore, the risk-based approach shall be regularly reassessed and updated when the risk factors associated with the financial institution change. The financial institution shall ensure that the risk-based approach is updated once every two years at a minimum or when risk factors change.

Chapter IX: The AML/CTF Guide

Section 1: ML/TF Risk Assessment

The main step for a financial institution to adopt a risk-based approach is to assess, understand and document its ML/TF risks and to identify the weaknesses that could be used to carry out ML/TF transactions. The risk assessment shall be comprehensive and include an analysis of the risks arising from:

Customers and beneficial owners;

The nature of products, services and transactions offered;
-countries or geographical regions in Saudi Arabia,

The channels used for providing services and products; and
Other risk factors.

The principles of this Guide do not aim to encourage financial institutions to reduce risks by excluding certain services or a certain class of customers due to the high risks associated with them as financial institutions are not prohibited from dealing with high-risk customers and business relationships. Rather, a financial institution shall develop and implement preventive risk mitigation measures commensurate with the results of the risk assessment it conducted.

Responsibilities of financial institutions to assess ML/TF risks are mentioned in Article (5) of the Anti-Money Laundering Law, Article (63) of the Law on Combating Terrorism Crimes and Financing, and Article (16) of its Implementing Regulations.

1.1 The financial institution shall take the appropriate steps to identify, assess, understand, and document in writing its ML/TF risks, provided that the nature and scope of the risk assessment are commensurate with the nature and size of the financial institution's business. Such risk assessment shall be updated regularly (once every two years at a minimum) and shall be documented and approved by the senior management. When carrying out the risk assessment process, the financial institution can focus on the following factors:

a) Risk factors associated with the financial institution's business, with an emphasis on:
   - Products and services.
   - Transactions.
   - Channels used for delivering services and products.
   - Countries or geographical areas within Saudi Arabia where the business of the financial institution or its subsidiaries, in which the financial institution owns the majority of shares, is conducted.

b) Risk factors associated with customers, beneficial owners, or the financial institution's beneficiary, with an emphasis on:
   - Products or services used by customers, beneficial owners, or beneficiaries.
   - The type of transactions executed by a customer.
   - The volume of deposits and transactions made by a customer.
   - Countries/geographical areas in which customers, beneficial owners, or beneficiaries conduct their businesses, or the source or destination of transactions.
   - Characteristics of a customer, beneficial owner, or beneficiary (e.g. Profession, age and type of legal entity).

c) Other risk factors, including:
   - ML/TF risks as issued by the Anti-Money Laundering Permanent Committee (AMLPC) and the Permanent Committee for Countering Terrorism (PCCT).
   - Results of the risk assessment issued by SAMA, competent authorities and other supervisory authorities, when available.

- Purpose of the account or business relationship.
- The frequency of transactions or duration of the business relationship.
- Attractiveness of products and services provided to money launderers including, but not limited to, private banking services and products offered to high net-wealth individuals as well as quick transfers to high-risk geographical areas.
- Regulatory risks associated with regulations and decisions issued by government entities.
- Business risks associated with the organizational and operational structure of the financial institution.
- ML/TF risks that may arise from the development of new products, business practices, or means of providing services, products or transactions, or those arising from the use of new technologies or technologies under development with new or existing products.
- Any additional risks arising from other countries with which customers are associated, including intermediaries and service providers.
- Any other variables that may increase or reduce the risk of ML/TF in a particular situation.
- Results of ML/TF risk assessments issued by international bodies and organizations such as the FATF, the Basel Committee, the World Bank, the International Monetary Fund, the United Nations, and Transparency International.

1.2 Before developing and implementing controls, policies and procedures to mitigate ML/TF risks, the financial institution shall determine its risk appetite with respect to the results of ML/TF risk assessment, taking into account regulatory, reputational, legal, financial, and operational risks.

1.3 The financial institution shall develop and implement controls, policies and procedures to mitigate ML/TF risks based on the risk assessment results referred to in Paragraph (1.1). The financial institution shall ensure that such procedures are effective, appropriate and sufficient to mitigate the risks associated with the assessment results. Furthermore, the financial institution

shall take into account that its activities will be exposed to risks regardless of the appropriateness and sufficiency of the measures taken. Therefore, it shall strengthen and update these measures whenever the need arises.

1.4 The financial institution shall classify all its customers according to the risk assessment results and take the necessary preventive measures to mitigate ML/TF risks. The financial institution can classify the level and degree of risks as (high, medium, or low) or using other categories as it determines based on the risk assessment results. This classification shall be consistent with the size and nature of the financial institution's business.

1.5 The financial institution shall review and update the customer risk profile regularly and based on the level of ML/TF risks.

1.6 The risk assessment shall be broad-based and at a level of sophistication commensurate with the business complexity of financial institutions with a complex organizational structure. For a financial institution with a less complex organizational structure, a simpler approach to conduct the risk assessment may be appropriate.

1.7 The financial institution shall assess risks before launching new products, services or business practices and before using new technologies or technologies under development, and it shall take appropriate measures to manage and reduce the identified risks as stated in Paragraph (1.3) under the ML/TF Risk Assessment Section.

1.8 The financial institution shall set up an appropriate mechanism for providing and submitting the information and reports on which the ML/TF risk assessment is based to SAMA upon request.

1.9 In the event that a customer is classified as high-risk, the financial institution shall obtain the senior management’s approval on the classification, provided that the information on which such classification is based is acceptable and reasoned.

1.10 Periodic reports shall be submitted to the board of directors regarding risk assessment at the level of the financial institution. The reports shall include the following:

a) Results of the ML/TF monitoring activities carried out by the financial institution.
b) The level of exposure to ML/TF risks based on major activities or customer categories.
c) General indicators and patterns of suspicious transactions as well as general trends and indicators of requests received from the SAFIU and the competent authorities.
d) Details of significant incidents, occurring internally or externally, and how they are handled in addition to their impact or potential effect on the financial institution.
e) Domestic and international developments in the AML/CTF laws, regulations, instructions and requirements as well as their impact on the financial institution.
f) The level of effectiveness of preventive measures in mitigating the effects of risks.

Section 2: Internal Policies, Procedures and Controls to Mitigate Risks

The development and implementation of a program for AML/CTF will be an effective and essential tool for applying the risk-based approach, provided that such a program should include controls, policies and procedures approved by the financial institution to mitigate ML/TF risks. The financial institution will have the discretion to determine the appropriate level of AML/CTF policies, procedures and controls, which shall be established based on the risk assessment results referred to under Section (1) of this Guide.

Article (14) of the Anti-Money Laundering Law and its Implementing Regulations and Article (18) of the Implementing Regulations of the Law on Combating Terrorism Crimes and Financing include the provisions and obligations that the financial institution shall include in its internal policies and procedures.

2.1 The financial institution shall develop an AML/CTF program that includes internal policies, procedures and controls to mitigate ML/TF risks in line with the risk assessment results approved by it as stated in Paragraph (1.1). The program shall also be documented, reviewed and enhanced continuously and approved at the level of the board of directors. Furthermore, the program should be commensurate with the nature and size of the financial institution's business.

2.2 The AML/CTF program shall include the detailed elements and strategic plans of the financial institution to ensure application of the AML/CTF requirements. This includes preparing and updating the AML/CTF policy based on the risk assessment results mentioned in Paragraph (1.1) under the ML/TF Risk Assessment Section in addition to developing and implementing relevant internal work procedures, including those related to due diligence/enhanced due diligence measures.

2.3 The financial institution shall include ,as a minimum, the following elements in its internal policy and procedures for combating ML/TF:

a) Due diligence, including enhanced and simplified due diligence measures.
b) Record keeping.
c) Monitoring and following up transactions and activities.
d) Reporting of suspicious transactions.
e) Arrangements of AML/CTF compliance function.
f) Independent audit function.
g) AML/CTF training.
h) Recruitment and follow-up criteria.

2.4 The AML/CTF policies, procedures and controls in the financial institution shall be clearly documented and communicated to all relevant employees in the financial institution departments. All the employees shall be adequately trained to implement such policies and procedures.

2.5 The AML/CTF program shall be applied by the financial group to all of its branches and subsidiaries in which it owns the majority shares. The policies and procedures of the financial group shall include the sharing of information among group members and the provision of customer and transaction information for the purpose of carrying out AML/CTF compliance or independent auditing tasks, provided that such information Should be kept confidential.

2.6 If the foreign host country of the company, in which the financial group or institution owns the majority shares, does not allow the implementation of the AML/CTF program in a manner consistent with the AML/CTF requirements in Saudi Arabia, the financial group or institution shall take the following preventive measures:

a) Implementing appropriate additional measures to manage ML/TF risks.
b) Submitting reports to the AML/CTF Department at SAMA on the gaps in the implementation of the program and on the additional measures taken to manage arising ML/TF risks.
c) Considering discontinuing of the subsidiary's operations if the financial group or institution is unable to put in place appropriate measures and procedures to mitigate ML/TF risks.
d) Adhering to any instructions received from SAMA in this regard.

Section 3: Due Diligence Measures

A. Due Diligence Measures

To establish a solid foundation for applying the risk-based approach, the financial institution shall know its customers and beneficial owners sufficiently to classify customer and business relationship risks from an AML/CTF perspective to direct its necessary resources to high-risk customers and business relationships to mitigate ML/TF risks. To achieve this objective, the financial institution shall classify customers based on the risks associated with them, as mentioned in the ML/TF Risk Assessment Section in this Guide. The information obtained from customers is the main basic tool for classifying customer risks. Therefore, the financial institution shall obtain reliable information from customers, verify such information, and ensure that it is updated and appropriate.

The volume of business that a financial institution is willing to accept should be matched with preventive measures that mitigate the risks associated with it. The financial institution is expected to develop a clear policy on customer and business acceptance and ensure that it has a sufficient level of internal controls to manage and mitigate ML/TF risks. Such preventive measures include the application of due diligence measures to identify and verify a customer, a person acting on his behalf, or a beneficial owner.

Article (7) of the Anti-Money Laundering Law and its Implementing Regulations and Article (17) of the Implementing Regulations of the Law on Combating Terrorism Crimes and Financing include the obligations of the financial institution upon application of due diligence measures.

3.1 The financial institution shall develop a policy for acceptance of new customers and business relationships, which includes due diligence measures to identify and verify a customer, a person acting on his behalf, or a beneficial owner. The policy shall be consistent with the risk assessment results and shall be documented and approved at the level of the board of directors.

3.2 The financial institution shall apply due diligence measures according to the type and level of risk posed by a certain customer, beneficial owner, or business relationship. Such measures shall be implemented in the following cases:

a) Prior to starting a new business relationship.
b) Prior to making a transaction for a natural or legal person with whom there is no business relationship, whether such transaction is carried out in a single operation or in several operations that appear to be linked.
a) Upon suspicion of ML/TF transactions.
b) When suspecting the credibility or adequacy of customer information previously obtained.
c) When a customer carries out a transaction inconsistent with his behavior or information.

3.3 At a minimum, due diligence measures shall comprise the following:

a) The financial institution shall identify the customer and verify the customer's identity based on documents, data or information received from an authenticated and autonomous source that is well known, reputable and trusted by the financial institution. In all cases, the source of information shall not be the financial institution or the customer, but rather an independent source. For example, information and documents issued by government bodies are considered to be from reliable and independent sources. Moreover, customer identification shall be made as follows[3]:
   - **Natural Person:** The person's full name according to official documents shall be obtained and verified in addition to the residence or national address, date and place of birth, nationality, and source of income.
   - **Legal Person:** The person's name shall be obtained and verified in addition to the information about its legal status, proof of incorporation, powers regulating and governing the legal person's work or the legal arrangement, names of all of its managers and senior executives, registered official address, place of business (if different), and the legal person's sources of revenue.

b) The financial institution should identify the person acting on behalf of the customer and verify its identity through an authenticated and autonomous source to ensure that such person is actually authorized to act in this capacity. Adequate measures shall be taken to identify the person acting on behalf of the customer, including the nature of business relationship between that person and the customer in addition to applying the measure set under Item (a).

c) The financial institution shall identify the beneficial owner and take adequate measures to verify the identity of the beneficial owner using documents, data or information from an authenticated and independent source as mentioned under the Beneficial Owner Section.

[3] Financial institutions must implement due diligence measures according to Paragraph (3.3) in addition to the relevant provisions in the Implementing Regulations of the Law on Supervision of Cooperative Insurance Companies, the Insurance Market Code of Conduct Regulations, the Implementing Regulations of the Finance Companies Control Law, the Implementing Regulations of the Financial Leasing Law, the Rules for Bank Accounts, the Rules Regulating Banking Agency in Saudi Arabia, the Regulations for Issuance and Operations of Credit and Charge Cards, the Regulatory Rules for the Prepaid Payment Services, and the Rules Regulating Money Changing Business.

d) The financial institution shall understand the purpose and nature of the business relationship and obtain additional related information if needed.
e) The financial institution shall understand the ownership and control structure of the (legal person) customer.

3.4 The financial institution shall develop the necessary procedures to collect sufficient information about customers and their expected use of products and services. The details and nature of the information are determined according to the degree and level of risks as high-risk customers and business relationships require greater scrutiny compared to those with lower risk. Therefore, the financial institution shall specify whether it should collect and verify any additional information based on the degree of risk posed by the customer and the business relationship.

3.5 The financial institution may choose not to carry out due diligence measures for each of the customer's transactions since it can rely on the information previously obtained in this regard, provided that such information is updated, appropriate, and not suspicious.

3.6 The financial institution shall not accept customers or business relationships or carry out transactions without knowing the name and verifying the information of the customer or beneficial owner. The financial institution shall not accept customers, establish business relationships, or carry out transactions under names consisting of numbers or codes or using anonymous or fictitious names.

3.7 The financial institution shall continuously apply due diligence measures to customers, business relationships, and beneficial owners based on the type and level of risk. It shall also verify transactions conducted throughout the business relationship in order to:

a) Ensure that the information of the customer or beneficial owner and their activities are consistent with the risks they pose.

b) Ensure that the documents, data and information obtained under the due diligence measures are up-to-date, appropriate, and consistent with the customer's activity and transactions.
c) Consider reporting a suspicious transaction to the SAFIU when there are sufficient grounds for the suspicion.
d) Reassess customers' risks based on their transactions and activities.
e) Verify business relationships and transactions of beneficial owners on a continuous basis.
f) Verify whether the customer is a politically exposed person (PEP).

3.8 The financial institution shall determine the number of times of reviewing and updating customer information based on the level and degree of risk posed by the customer, provided that due diligence measures are carried out continuously and more frequently for high-risk customers along with the appropriate enhanced measures.

3.9 The customer is not required to come to the financial institution when updating and reviewing their information for identity verification as long as electronic authentication services approved by the National Information Center are used. However, the financial institution shall determine the need for further documentation or the customer's presence based on the level of risk posed by the customer.

3.10 When using reliable and independent electronic services to verify a customer's identity, the financial institution shall determine if more documentation is required based on the level of risk posed by the customer. In addition, it must implement the necessary preventive measures to mitigate business relationship risks and set the necessary procedures and measures to verify and review the customer information obtained, including the information provided by the customer, using reliable and independent electronic services.

3.11 The financial institution shall take all the measures required to update and review information of customers and beneficial owners. If its preventive measures are found to be unsuccessful, this shall be clarified and documented as stated in Paragraph (6.6) in the Record Keeping

Section. If the financial institution is unable to comply with the due diligence requirements, it must not establish a business relationship or execute a transaction for a customer. If an existing business relationship or customer is involved, the financial institution shall terminate the related business relationship and consider reporting suspicious transactions to the SAFIU.

3.12 The financial institution shall develop effective procedures to verify all the names of customers and beneficial owners, including all managers, senior executives, owners, and persons acting on behalf of customers, and compare them with those included in the sanction lists by local authorities and the United Nations before or during a business relationship or a transaction, taking into account Paragraph (8.15) in the Reporting of Suspicious Transactions Section.

3.13 The financial institution shall follow up on the available sanction lists of other countries[4], verify all transactions and transfers, and use these lists for comparison in order to avoid potential legal problems that the financial institution or any other local or international parties might face and to avoid freezing of customer transactions or transfers.

3.14 In the event of suspicion of a ML/TF operation and when the financial institution has strong justifications and reasonable grounds that the customer may become aware of the suspicion upon application of the due diligence measures, the financial institution shall decide, at its discretion, not to carry out due diligence, provided that it shall comply with Paragraph (8.8) in the Reporting of Suspicious Transactions Section.

3.15 The financial institution shall use the best technologies to identify and record information in accordance with the due diligence requirements, so that changes in the data and their dates can be monitored and identified. Recorded and entered information shall be correct and consistent with the

[4] Such as the sanctions lists of the European Union, the Office of Foreign Assets Control (OFAC) of the US Treasury Department, the US State Department, Interpol, etc.

information provided by the customer after being verified. This shall include:

a) Information of customers.
b) Information of beneficial owners.
c) Information of owners and all managers and senior executives of the customer.
d) Information of the person acting on behalf of the customer.

3.16 The financial institution may accept the execution of a transaction for an occasional customer who does not have a business relationship with it. This applies to individuals (citizens and residents) and visitors with a visa of temporary residence, taking into consideration Paragraph (4.4) in the Enhanced Due Diligence Section.

B. Beneficial Owner

To implement the risk-based approach, the financial institution shall be certain of the identity of the beneficial owner or any person controlling the business relationship. The beneficial owner may not be a legal person, but rather a natural person who owns or controls the legal person directly or indirectly.

Concealing ownership information related to business and operations is one of the methods used for ML/TF. Therefore, collecting the necessary information and verifying the identity of the beneficial owner or anyone controlling the business relationship is important in combating ML/TF.

Article (7/3) of the Implementing Regulations of the Anti-Money Laundering Law and Article (17) of the Implementing Regulations of the Law on Combating Terrorism Crimes and Financing stipulate the measures that must be taken by the financial institution to identify and know the beneficial owner.

3.17 The financial institution shall know the identity of the beneficial owner and take sufficient and appropriate measures to verify that identity, using documents, data or information from an authenticated and independent source. In order to verify the beneficial owner's identity, the financial institution shall obtain and review all necessary details and information,

provided that the due diligence measures taken by the financial institution shall be consistent with the degree and level of risk.

3.18 The financial institution shall know the identity of the natural person who owns or controls (25%) or more of the legal person's shares and take sufficient and reasonable measures to verify that identity, taking into account that a natural person who controls (25%) of the shares may not necessarily be the beneficial owner. In this case or when there is no natural person who owns or controls (25%) or more of the legal person's ownership, or if there is suspicion that the owner of the controlling share is not the beneficial owner, the financial institution may take the following preventive measures:

a) Identifying the natural persons who occupy senior management positions with the legal person, so that the financial institution becomes sufficiently satisfied that these persons control the legal person.
b) Identifying the owners who control less than (25%) of the shares if it becomes clear to the financial institution that these owners are the beneficial owners or controlling the legal person.
c) Identifying the natural person who holds the position of senior management officer.
d) Identifying the high-risk customer and taking preventive measures, including enhanced due diligence measures and continuous monitoring of the customer.
e) Keeping records of the measures and procedures taken by the financial institution in addition to the reasons for suspecting that the owner of the controlling share is not the beneficial owner.

3.19 The financial institution shall not rely primarily on the written statement of a customer to identify the beneficial owner; it shall take reasonable and adequate measures to verify the beneficial owner by understanding the ownership and control structure of the legal person. In order to understand that structure, the financial institution can refer to any of the following documents:

a) The data of joint stock companies listed on the Capital market.
b) The stockholders register.
c) The memorandum of association.
d) Minutes of board meetings.
e) The company's commercial register.
f) The articles of association.

3.20 The financial institution shall maintain records and documents related to the identification and verification of the beneficial owner as mentioned in Paragraph (6.1) of the Record Keeping Section.

3.21 If the customer of the financial institution is an individual, it shall ensure that the business relationship with that customer is used for the benefit of the individual whose name is registered and for the purposes specified (and determine whether the customer is acting in his own interest). In the event that there is a suspicion that the customer is acting in the interest of others, the financial institution must specify the capacity in which the customer, or anyone acting on his behalf, acts. The beneficial owner is then identified to the satisfaction of the financial institution. It shall also ensure that any person claiming to act on behalf of a customer is authorized and shall identify and verify that person's identity.

C. Reliance on a Third Party to Implement Due Diligence Measures

The financial institution may rely on another financial institution or any of the owners of DNFBPs to implement the due diligence measures. However, when a financial institution carries out the due diligence measures itself, it will be in a better position to identify and assess customer risks, especially when such measures involve meeting customers in person.

In all cases, in accordance with the obligations mentioned in the Anti-Money Laundering Law, the Law on Combating Terrorism Crimes and Financing, and their Implementing Regulations, the responsibility for implementing due diligence measures shall rest with the financial institution seeking assistance from another party as such financial institution is fully responsible for complying with the regulatory requirements relating to due diligence and SAMA's Instructions for Outsourcing.

Article (7/10) of the Implementing Regulations of the Anti-Money Laundering Law allows the financial institution to rely on another financial institution or any of the owners of DNFBPs to carry out the due diligence measures, including entities that are part of the same financial group. Articles (7/11) and (7/13) of the Implementing Regulations specify the conditions that must be fulfilled by the financial institution prior to reliance on another party.

3.22 The financial institution may rely on a third party, whether it is a financial institution or any of the owners of DNFBPs, to implement the due diligence measures, in accordance with the following:

a) The financial institution shall ensure that the third party is subject to regulation and supervision and that it applies due diligence and record-keeping measures as stated in the Anti-Money Laundering Law, the Law on Combating Terrorism Crimes and Financing, and their Implementing Regulations.
b) The financial institution shall take actions to ensure that due diligence information is provided by the third party upon request and without delay.
c) The financial institution shall immediately obtain all information related to due diligence, including simplified and enhanced due diligence measures, from the third party.
d) The financial institution shall take into consideration the information available to the AMLPC, the PCCT, and the SAFIU on high-risk countries when determining the countries in which the third party may be conducting business.

3.23 The financial institution shall assess the ML/TF risks associated with reliance on a third party and, therefore, it shall develop and apply appropriate policies and procedures for risk management. Such procedures may include the following:

a) Identification of the minimum due diligence requirements to be met by the third party.
b) Conduct frequent examination of obtained information and documents to apply the due diligence measures, including enhanced or simplified due diligence.

c) Monitoring of customers and business relationships established them through reliance on a third party as well as application of intensive control measures towards them in accordance with the ML/TF risk assessment results.

3.24 The financial institution shall periodically verify (at least annually) that the third party has the sufficient capabilities and powers required to fulfill the due diligence requirements in a professional manner. The financial institution shall also continuously assess the third party's compliance with such requirements.

3.25 The financial institution has the right to directly obtain the customer due diligence information from the third party relied upon to perform due diligence, if such party has previously implemented due diligence measures for the same customer when dealing with another financial institution, taking into account that the required information shall be complete and that due diligence measures are constantly applied according to the requirements mentioned in Paragraph (3.7) in the Due Diligence Section.

Section 4: Enhanced Due Diligence Measures

A. Enhanced Due Diligence Measures

Customer classification according to the level of risks is a key element in the financial institution's risk-based approach. The financial institution shall identify the risk factors to be taken into consideration when classifying a customer in the high-risk customer category from the AML/CTF perspective. It shall also take additional steps to collect information about high-risk customers and business relationships in order to understand and assess risks and monitor transactions more accurately. It is the responsibility of the financial institution to identify high-risk customers, either individually or by category, and accordingly implement enhanced due diligence measures in a manner that ultimately leads to mitigating risks.

The financial institution may also refer to a set of available resources to classify the degree and level of risk for high-risk customers, including the data collection form prepared by SAMA and the FATF guidelines

that aim to assist financial institutions in identifying high-risk customers.

Article (7/14) of the Implementing Regulations of the Anti-Money Laundering Law and Article (17) of the Implementing Regulations of the Law on Combating Terrorism Crimes and Financing state that it is the responsibility of the financial institution to implement enhanced due diligence measures in the case of ML/TF high risks based on the type and level of risk posed by a specific customer or business relationship. Article (11) of the Anti-money Laundering Law and Article (66) of the Low on Combating Terrorism Crimes and Financing require the financial institution to apply enhanced due diligence measures commensurate with the risks involving business relationships and transactions with a person from a country identified as a high-risk country by the financial institution, the PCCML, or the PCCT.

4.1 The financial institution shall design and implement its risk-based approach in a manner that enables it to identify high-risk customers and beneficial owners according to the risk elements specified in Paragraph (1.1) in the ML/TF Risk Assessment Section. When a customer or business relationship is classified as high risk, the financial institution shall take enhanced risk mitigation measures, including enhanced due diligence measures.

4.2 The financial institution shall include in its approved AML/CTF policies and procedures the enhanced due diligence measures to be taken to identify high-risk customers and business relationships. These measures may include the following:

a) Obtaining and verifying information about the customer's job, activity or profession.
b) Identifying and knowing the source of funds/income at the beginning of dealing with the customer and when carrying out transactions for the customer as well as verifying the data and information.
c) Obtaining information regarding the customer’s size of assets and transactions.

d) Conducting on-site visits to verify the nature of the customer's business.
e) Obtaining any additional documents or information to know the customer.

4.3 Upon identifying a high-risk customer before/after establishing the business relationship, the financial institution shall obtain approval from the senior management to deal with and continue the business relationship with the customer.

4.4 The financial institution shall apply enhanced due diligence measures to high-risk customers and business relationships with any natural or legal person, even if the financial institution does not have a business relationship with that person, if such person poses high risk from the AML/CTF perspective.

4.5 When discovering that another financial institution has refused to deal with a specific customer, the financial institution shall implement enhanced due diligence measures, know the reasons behind that refusal, and take additional due diligence measures if the reason for refusal was a suspicion related to ML/TF.

4.6 The financial institution shall apply enhanced due diligence measures to customers with a complex organizational structure so it can understand and identify customer risks and verify the beneficial owner.

4.7 The financial institution shall take appropriate measures to identify high-risk countries associated with ML/TF risks and implement enhanced due diligence measures that are commensurate with the risks that may arise from business relationships and transactions with a person from such countries. This includes the following:

a) Following up what is issued by the PCCML regarding high-risk countries.
b) Following up what is issued by the PCCT regarding high-risk countries.
c) Following up on the guidance issued by the FATF concerning the deficiencies of countries in the implementation of preventive

measures to protect the international financial system against ML/TF risks.

4.8 When taking enhanced customer due diligence measures, the financial institution shall properly document these measures in accordance with Paragraph (6.1) in the Record Keeping Section.

B. Politically Exposed Persons (PEPs)

Identifying a PEP and the extent to which that person is considered politically exposed is one of the customer due diligence measures taken by the financial institution to implement the risk-based approach in conducting its business. The political influence and power of such person may lead to misuse of this power for illicit enrichment. Proceeds in this case are often transferred under names of relatives or persons close to a PEP for the purpose of concealment.

Therefore, the financial institution shall take reasonable measures to identify whether a customer or beneficial owner is a PEP. In cases of high-risk business relationships with PEPs, the financial institution shall apply enhanced due diligence measures and apply the same to all types of PEPs, their family members, and persons close to those PEPs.

Article (8) of the Anti-Money Laundering Law and its Implementing Regulations require the financial institution to develop internal procedures and provide appropriate tools to identify PEPs and implement enhanced due diligence measures regarding them.

4.9 The financial institution shall use appropriate tools and measures to determine if a customer or beneficial owner is a PEP, whether that person is foreign or local. These tools and measures may include the following:

a) Searching for the customer in any available information sources.
b) Relying on a credible database to identify and verify the information of PEPs, including the use of programs or information systems that enable the financial institution to determine if a customer, potential customer, or beneficial owner is a PEP.
c) Include specific questions regarding a customer being a PEP at the start of the business relationship or when updating and reviewing customer information.

d) Verify the customer's position and the potential use of power related to it.

4.10 The financial institution shall take into consideration that mere reliance on electronic systems and programs does not guarantee full compliance with the Anti-Money Laundering Law and its Implementing Regulations. The financial institution is responsible for determining whether a customer is a PEP or not, and combining the tools mentioned in Paragraph (4.9) may be highly effective in identifying and verifying the PEP.

4.11 The financial institution shall determine if a customer or beneficial owner is a PEP in the following cases:

a) Prior to starting a new business relationship.
b) Prior to making a transaction for a natural or legal person with whom there is no business relationship, whether such transaction is carried out in a single operation or in several operations that appear to be linked.
c) When updating or reviewing customer information.
d) Upon suspicion that the customer is a PEP.

4.12 The financial institution shall continuously apply due diligence to customers, business relationships, and beneficial owners to verify if a customer is a PEP, as mentioned in Paragraph (3.7) in the Due Diligence Section.

4.13 The financial institution shall classify the foreign person as a high-risk PEP customer and implement enhanced due diligence measures to mitigate risks, including:

a) Obtaining approval of the senior management before establishing or continuing a business relationship with that person.
b) Taking all reasonable measures to identify the source of the customer's wealth and funds.
c) Implementing enhanced and continuous due diligence measures for the business relationship.

The financial institution shall apply the same measures to local PEPs when the level of ML/TF risks is high.

4.14 The financial institution shall apply the same enhanced due diligence measures to the family members of the PEP as well as any person close to the PEP.

4.15 To determine the level and degree of risk posed by a local PEP, the financial institution shall observe the requirements mentioned in Paragraph (1.1) under the ML/TF Risk Assessment Section. It may also rely on the following information:

a) The period of time for which a local PEP has been entrusted with prominent public functions in Saudi Arabia or in a foreign country.
b) Corruption risks associated with the entity where a local PEP occupies his position and the extent to which that entity is exposed to corruption risks.
c) The customer's attempt to conceal or present inaccurate information related to the application of due diligence/enhanced due diligence, such as:
   - Concealing or providing inaccurate information related to the customer's job and the extent to which it is associated with high public positions or functions in Saudi Arabia or any foreign country.
   - Concealing or providing inaccurate information related to the source of income/wealth.
d) Reliance on the family members of a local PEP or persons close to that person to act on his behalf.

4.16 The financial institution shall have sufficient, reasonable and documented grounds based on the ML/TF risk assessment results if it decides that a local PEP, their family members, or persons close to that PEP do not pose high risk from the AML/CTF perspective.

4.17 If it is established from protection and/or savings policies or investment-related insurance documents that a beneficiary or beneficial owner is a

PEP, the financial institution shall take enhanced due diligence measures to mitigate risks before the payment of benefits or exercise of any rights under those documents. Such measures shall include the following:

a) Notifying the senior management before the payment of benefits or exercise of any rights under those documents.
b) Carrying out a thorough examination of the business relationship with the customer and considering reporting to the SAFIU in case of a suspicious transaction.

The rights exercised by a customer under a policy may include:

- Cancellation of the policy.
- Cancellation of the policy during the free-look period.
- Partial withdrawal of the investment amount.
- Change of investment fund.
- Payment of additional premiums.

4.18 If the financial institution fails to identify a PEP or has suspicions regarding a PEP, it shall include the following in its records:

a) The measures taken to determine the customer type.
b) Reasons for suspicions about the nature of the customer's position or job or association with a PEP.
c) Reasons why the measures did not work.
d) The date on which the measures were taken.

Section 5: Simplified Due Diligence Measures

The financial institution's adoption of the risk-based approach can result in identifying and classifying customers and business relationships of low risk from the AML/CTF perspective. Thus, it is possible for the financial institution to implement simplified measures in cases where the ML/TF risk assessment results indicate low risk.
In order for the financial institution to reach such result, sufficient information about the customer must be collected to determine the related level of risk.

Article (5/5) of the Implementing Regulations of the Anti-Money Laundering Law and Article (17) of the Implementing Regulations of the Law on Combating Terrorism Crimes and Financing state that the financial institution may apply simplified measures when the ML/TF risks are low subject to the necessary conditions.

5.1 When the level of ML/TF risks is low, the financial institution may take simplified measures, provided that there is no suspicion of any ML/TF transaction. Such simplified measures shall be commensurate with the low risks and must include the adoption of simplified due diligence to identify and verify the customer's identity.

5.2 The financial institution shall include the simplified measures and procedures applied to low-risk customers and business relationships in the approved AML/CTF policies and procedures.

5.3 Application of the simplified measures does not mean exemption from the requirements of customer due diligence, but rather the application of due diligence measures in a streamlined and simplified manner consistent with the ML/TF risks posed by the customer or beneficial owner. Regardless of the level of risk posed by the customer or business relationship, the financial institution shall comply with the following when applying due diligence:

a) Verifying the identity of the customer or the person acting on his behalf, relying on an authenticated and independent source.
b) Identifying and verifying the identity of the beneficial owner through a reliable and independent source to the satisfaction of the financial institution that it knows the beneficiary owner.
c) Understanding the nature and purpose of the business relationship.
d) Understanding the ownership and control structure of the customer who is a legal person.

5.4 The financial institution may apply simplified due diligence measures for all the criteria mentioned in Paragraph (5.3) in the Simplified Due Diligence Section. The financial institution determines the nature and quality of these simplified due diligence measures according to its

ML/TF risk assessment results. Such measures are usually associated with the following elements:

a) Timing of verification of the customer's information and associated documents.
b) The intensity and periodicity of the verification of customer information.
c) Details and nature of the information obtained from the customer.

5.5 Having identified the customer, the financial institution may postpone the identity verification process, provided that it shall adhere to the following:

a) Verifying the information and documents of the customer as soon as possible.
b) Ensuring that it is necessary to postpone the verification of the customer's identity to avoid interruption of usual business procedures.
c) Applying appropriate and effective measures to control ML/TF risks.
d) Ensuring that measures for risk management are in place regarding the situations in which a customer can benefit from a business relationship prior to the verification process.

5.6 If simplified due diligence measures have been applied to certain customers and business relationships, they shall be subjected to monitoring by the financial institution, as described in Paragraph (7.3) in the Monitoring of Transactions and Activities Section. Based on continuous monitoring, the financial institution shall consider applying enhanced due diligence in the case of high ML/TF risks.

5.7 When carrying out a transaction for an occasional customer, the financial institution shall obtain the information of the identity of the citizen/resident or the passport and visa information of the visitor/temporary resident and record the executed transactions number as a reference. If the transaction involves a money transfer or check, a copy of the ID or passport and visa shall be obtained and the requirements under the Wire Transfer Section shall be met.

5.8 An occasional customer is allowed to execute the following transactions:

a) Payment of utility bills.
b) Payment of amounts payable to government entities.
c) Currency exchange, money transfer, and cashing of checks with a maximum amount of SAR 5,000 or its equivalent per transaction, or no more than SAR 50,000 or its equivalent in one year.
d) Purchase of visitor mandatory insurance policies.

Section 6: Record Keeping

The financial institution shall make its records available to the competent authorities and to its relevant departments in order to allow analysis of data, tracking and structuring of financial transactions, tracing of the origin and executor of transactions as well as those authorized to sign or carry out transactions.

Article (12) of the Anti-Money Laundering Law and Article (65) of the Law on Combating Terrorism Crimes and Financing state the financial institution's obligations relating to the manner of record keeping, the minimum record-keeping period, and the possibility for extending that period according to the regulatory requirements.

6.1 The financial institution shall keep records for a period of no less than ten years from the date of the end of the business relationship or contract, conclusion of the transaction, or closure of the account, or the date of completion of a transaction for a customer who has no business relationship with the financial institution (occasional customer). The financial institution shall also comply with any instructions issued by the competent authority to extend the record-keeping period.

6.2 The financial institution shall put in place approved internal procedures and controls for record keeping and documentation and ensure that they are reviewed and enhanced on an ongoing basis and effectively implemented. These shall at least include the following:

a) The manner for record keeping (paper or electronic) and the mechanism and authorization for access to records and their retrieval.

b) The measures taken to meet the regulatory requirements related to record keeping outside Saudi Arabia to ensure that there are no obstacles to having access to the records.
c) Arrangements of the record keeping department that ensure meeting the regulatory requirements for AML/CTF.

6.3 The financial institution shall provide the record keeping department with adequate resources, take the necessary measures to maintain and protect its electronic archiving systems, and conduct periodic tests (at least annually) to verify the effectiveness of the record-keeping process.

6.4 The financial institution shall keep records in a retrievable and auditable manner and maintain a complete and appropriate status of the records to allow analysis of data and tracking of transactions, provided that the financial institution provides SAMA with the necessary records as requested.

6.5 In the case of outsourcing, the financial institution should consider the following:

a) The contract must clearly state the obligations requiring the third party to enable the financial institution to obtain records and exercise the right to directly access the data related to outsourcing in addition to the right of access to the service provider's workplace.
b) The contract must clearly state the obligations requiring the third party not to provide any other party with the data or records or allow access to the areas or technological systems used for document and record keeping, except through the financial institution after coordination with SAMA.
c) The financial institution shall conduct periodic checks by asking the third party to provide various samples of the records to ensure that the third party is compliant with the obligations and requirements of the contract in line with the regulatory requirements.
d) The requirements stated in Paragraphs (3.21) and (3.22) in the Due Diligence Section shall be observed.

6.6 When unsuccessful preventive measures have been taken by the financial institution, it shall keep a document explaining these measures for no less than ten years from the date on which the measures were taken, provided that the document includes the reasons why the measures did not work. In all cases, the financial institution shall observe Paragraph (3.11) under the Section on Due Diligence Measures.

6.7 The financial institution shall keep documents related to internal investigations, inspections, and suspicious activity reports for a period of no less than ten years from the date of reporting to the competent authorities or taking the decision not to report, taking into account that:

a) Reports and internal investigations shall be confidential.
b) Specify employees authorized to have access to the documents.

6.8 When conducting wire transfers, the financial institution shall maintain all information related to the wire transfer originator and the beneficiary as stated under the Record Keeping Section.

6.9 In cases of wire transfers outside Saudi Arabia, the intermediary financial institution in the payment chain shall ensure that all information relating to the originator and beneficiary remains with the wire transfer and shall keep all of that information in its records as stated under the Record Keeping Section.

6.10 In cases where technological restrictions prevent the retention of information about the originator or beneficiary associated with a wire transfer outside Saudi Arabia and it is intended to be kept with the relevant local wire transfer data, the intermediary financial institution shall keep a record containing all information received from the financial institution that originated the transfer or from the intermediary institution for a period of ten years from the date of completion of the transaction or closure of the account.

Section 7: Monitoring of Transactions and Activities

The monitoring of transactions and activities, including those unusual and suspicious, is an important element for applying the risk-based approach as it enables the financial institution to identify and report any suspicious transactions or activities to the SAFIU. In addition, monitoring systems in the financial institution allow continuous assessment of preventive measures and controls as well as enhancement of their efficiency by making use of any unusual activities detected that led to suspicion of ML/TF.

Article (13) of the Anti-Money Laundering Law and Article (69) of the Law on Combating Terrorism Crimes and Financing state the financial institution's responsibilities to continuously monitor transactions, documents and data to ensure that they are consistent with the information the financial institution has about the customer or business relationship. These responsibilities also include giving particular attention to unusual transactions and activities, especially when they involve high ML/TF risks.

7.1 The financial institution shall put in place measures and procedures based on the risk assessment results to monitor transactions and identify unusual transactions and activities. The measures and procedures shall be effectively implemented and documented by the financial institution; and approved at the senior management level.

7.2 When developing the oversight measures and procedures, the financial institution shall apply a risk-based monitoring approach according to the degree and levels of risk derived from the ML/TF risk assessment results. This risk-based monitoring approach shall enable the financial institution to:

a) Implement enhanced measures by improving the process and degree of oversight on high-risk customers and transactions, including:
   - Review and monitoring of high-risk transactions.
   - Frequent monitoring of the activities and transactions of high-risk customers in addition to preparing relevant

reports and frequently carrying out the required internal investigations.

- Tracking and financial analysis of unusual activities or transactions carried out by customers.

b) Implement simplified measures for low-risk customers and businesses, including reducing the rate and frequency of monitoring in the case of low ML/TF risk.

7.3 Carrying out simplified oversight on low-risk customers and businesses does not mean exemption from the requirements of monitoring as the financial institution shall monitor all customers and transactions on an ongoing basis. However, it allows the financial institution to implement control procedures in a streamlined and simplified manner consistent with the ML/TF risk posed by the customer or business relationship in order to be able to focus its resources on high-risk customers and transactions.

7.4 To apply the risk-based oversight approach, the financial institution shall observe the following:

a) The financial institution shall provide supervisory tools commensurate with the risks identified in accordance with Paragraph (1.1) under the ML/TF Risk Assessment Section, to enable it to analyze and detect unusual transactions, patterns, and activities in real time of execution or before that. The financial institution shall provide adequate human resources in this regard to monitor transactions and activities and detect any unexpected or unusual behavior from customers. Such tools shall be consistent with the nature, size, and complexity of the financial institution's business and it shall ensure adequate and continuous monitoring.

b) The financial institution shall develop indicators and patterns commensurate with the risks identified, the complexity of its business and activities, and modern ML/TF technologies so that it can detect unusual transactions or activities according to the requirements, development and diversity of the methods used in the execution of such operations and transactions. The indicators can

be transformed into strategies for assessing ML/TF risks and designing controls to mitigate such risks.

7.5 The supervisory tools of the financial institution shall include appropriate technological systems that enable it to monitor transactions and activities and detect any unusual or unexpected behavior from customers as manual monitoring of transactions alone is not sufficient. It is necessary for the financial institution to use effective electronic systems for its continuous oversight of transactions, and the systems used shall be commensurate with its risk complexity and outcomes. However, these systems shall be integrated with the basic systems of the financial institution to achieve the following:

a) Linking the risk-based customer classification to the technological system to allow further monitoring of high-risk customers and transactions in accordance with the requirements stated in Paragraph (7.2) in the Monitoring of Transactions and Activities Section.
b) Following-up all the business of the financial institution as appropriate to ensure adequate monitoring and control.
c) Applying a simplified monitoring approach consistent with the risks posed by low-risk customers and businesses, in accordance with Paragraph (7.2) under the Monitoring of Transactions and Activities Section.

7.6 The financial institution shall test the supervisory tools periodically (Once a year a maximum) to ensure that they are effective and adequate and shall develop these tools based on the results of periodic tests that must be documented.

7.7 The financial institution shall monitor customers and transactions on an ongoing basis and take the necessary preventive measures to review and update customer information and categorize customers based on the monitoring results, in accordance with Paragraph (3.7) in the Due Diligence Section. This is to detect any inconsistency between the information disclosed by customers at the beginning of or during a business relationship and the activities monitored. Customers and

transactions shall continue to be monitored until the conclusion of the business relationship.

7.8 The financial institution must qualify and train its employees to carry out the monitoring process according to their various work tasks and it shall not only rely on technological systems and programs, taking into consideration its prescribed ML/TF indicators.

7.9 The financial institution shall develop indicators and typologies commensurate with the nature and risks of its business that point to the suspicion of ML/TF transactions, taking into account the diversity and development of ML/TF methods. Moreover, the financial institution shall constantly update these indicators as required and according to development and diversity of the methods used for ML/TF. It shall also observe the instructions issued by SAMA, the PCCML, or the PCCT and those issued by other local or international bodies, such as the FATF.

7.10 The financial institution's key positions/posts that might be targeted for ML/TF purposes shall be identified. The financial institution shall closely monitor those holding these positions and ensure that they consistently implement AML/CTF policies and procedures.

Section 8: Reporting of Suspicious Transactions

The financial institution shall set up and effectively implement internal procedures for reporting unusual transactions or activities to protect itself from being exploited as a channel to carry out ML/TF transactions. The financial institution shall have a database that helps employees determine if unusual transactions or activities provide reasonable grounds to suspect ML/TF.

Articles (15) and (16) of the Anti-Money Laundering Law and Articles (70) and (71) of the Law on Combating Terrorism Crimes and Financing set forth the financial institution's obligations to report suspicious transactions in addition to the regulatory requirements related to non-alerting customers .

8.1 The financial institution shall set up and document procedures for reporting suspicious transactions, implementing them effectively, and ensuring that they are approved at the level of the board of directors. The procedures may include the following:

a) Internal procedures to be followed by the its employees and senior officers in the event of suspicion of ML/TF.
b) A mechanism that facilitates employees' communication with the officer responsible for reporting suspicious transactions to raise inquiries and report suspicions.
c) Internal investigation procedures relating to suspicion cases, including the stages of investigation.
d) Levels of approval and review of suspected cases if reports are approved or closed.
e) Determining the employee or officer responsible for reporting to the SAFIU about suspicious transactions.
f) Adequate measures to maintain confidentiality of reports and ensure that customers are not alerted.

8.2 The financial institution shall provide sufficient resources that allow effective follow-up and sufficient investigations of all internal reports to determine whether submitting a suspicion report to the SAFIU is justified.

8.3 The financial institution shall immediately and directly inform the SAFIU upon suspicion or the presence of information or reasonable grounds to suspect that a customer's behavior is related to ML/TF acts. If the financial institution submits a report to the SAFIU, it shall respond to and provide the SAFIU with any additional information that it requests directly in order to analyze the submitted report.

8.4 The financial institution shall report all suspicious transactions, including unsuccessful attempts to carry out transactions, if there are reasonable grounds for suspicion, regardless of the transaction's value.

8.5 The financial institution shall inform the SAFIU upon suspicion of wire transfer transactions.

8.6 The financial institution shall not submit any report to the SAFIU based on speculation or lack of information or reasonable grounds for suspicion. The financial institution has reasonable grounds to report on suspicions in the following cases:

a) When the financial institution knows, through its conduct of its business or investigations, that the activity or operation to be carried out is related to a suspicious transaction.
b) When the financial institution has sufficient information indicating that the activity or transaction to be carried out is related to a suspicious transaction.

8.7 The financial institution shall decide, at its discretion, not to apply the due diligence measures in the event of suspicion of an ML/TF act when it has strong justifications and reasonable grounds that the customer may become aware of the suspicion if the financial institution applies due diligence. In this case, it shall submit a report on a suspicious transaction to the SAFIU. The report shall include the reasons and justifications for not applying due diligence.

8.8 The financial institution shall submit suspicious transaction reports according to the reporting mechanism and form approved by the SAFIU, on the condition that the SAFIU is provided with an additional detailed report that includes all data and information available to the financial institution on that transaction and the parties involved.

8.9 The financial institution shall submit a technical report on the reported cases to the SAFIU. The report shall include the following:

a) The account statement or transactions carried out under the contract for a period of six months.
b) Documents obtained to apply due diligence measures.
c) A technical report examining the account or contract subject of suspicion.

8.10 If a decision not to inform the SAFIU of an internal report is made, the officer responsible for reporting suspicious transactions shall document

this including the reasons for not reporting in a detailed and sufficient manner, taking into account the levels of approval and review mentioned under Paragraph (8.1/d).

8.11 The financial institution shall keep records of all suspicious transaction reports submitted, including a copy of reports submitted to the SAFIU and internal reports on cases that were under investigation and were not reported due to the lack of sufficient grounds for suspicion. Investigation documents and reports shall be kept independently without prejudice to the requirements of confidentiality of investigations and reports, and the persons authorized to access these records shall be specified.

8.12 The financial institution shall examine and review suspicion cases, internal reports, and feedback received from the SAFIU and take them into account when developing/updating the indicators and typologies of ML/TF mentioned in Paragraph (7.9) in the Monitoring of Transactions and Activities Section.

8.13 The financial institution should educate and raise the awareness of all its employees, including the members of the board of directors and senior management, regarding the following:

a) The requirements related to identifying and reporting the suspicious activity or transaction.
b) The regulatory requirements concerning civil and criminal liability and other liabilities related to violations of required confidentiality obligations.
c) The regulatory requirements related to reporting and not alerting customers or disclosing any suspicious transaction incidents, reports or information.

8.14 The financial institution shall notify SAMA immediately of any accounts, business relationships, or financial transactions involving the names included in the lists of the UN Security Council committees, Committee 2253/1989/1267 and Committee 1988, as well as the names included in the national list in implementation of the Security Council Resolution No. (1373) according to the data available in the lists. For

optimal implementation, the financial institution shall adhere to the provisions of SAMA's relevant circulars, including:

a) The Guide on the Implementation of Security Council resolutions relevant to combating terrorism and its financing.
b) The Guide on the Implementation of Security Council resolutions relevant to proliferation of weapons of mass destruction and financing.

8.15 The financial institution shall put in place an effective and comprehensive mechanism and consider the suitability of technological systems for continuous comparison with the names included in the sanctions list in Paragraph (8.14) under the Reporting of Suspicious Transactions Section.

Section 9: Arrangements of AML/CTF Compliance Function

In order for the financial institution to implement the risk-based approach effectively and adequately, its board shall provide sufficient resources, including human and technological resources that are commensurate with the nature and volume of the financial institution's business and the risk assessment results to combat ML/TF so as to ensure the effective implementation of AML/CTF internal policies, procedures and controls. This shall include setting up appropriate arrangements at the level of the financial institution and appointing an officer for the AML/CTF compliance function with specified work duties. The AML/CTF compliance function shall be an administrative and technical reference for the board and a sub-reference for the senior managements.

Article (14/1) of the Implementing Regulations of the Anti-Money Laundering Law and Article (18) of the Implementing Regulations of the Law on Combating Terrorism Crimes and Financing set forth the obligations of the financial institution, which include setting up appropriate AML/CTF arrangements.

9.1 The financial institution shall set up appropriate arrangements for the AML/CTF Compliance Unit/department, which shall at least include the following:

a) The AML/CTF compliance function.
b) Appointing the person responsible for the AML/CTF compliance function at the senior management level.
c) Ensuring that the officer responsible for the AML/CTF compliance function works independently and administratively and technically reports to the board of directors and its committees.
d) The officer responsible for the AML/CTF compliance function shall have the power to have timely access to any information, including customers' data under the due diligence measures, records of other related transactions, or any data necessary to carry out all his work.

9.2 The financial institution shall establish an independent and specialized AML/CTF unit and provide it with sufficient resources, including human and technological resources, to carry out its work perfectly as well as the necessary professional competence and capabilities when recruiting qualified personnel to occupy positions in the AML/CTF unit that shall be solely restricted to Saudi nationals.

9.3 The financial institution shall specify the duties and responsibilities of the AML/CTF compliance function officer approved in job description. The responsibilities shall include all AML/CTF work, such as the following:

a) Developing an AML/CTF program commensurate with the volume and nature of the financial institution's business and the ML/TF risks it has identified in order to reduce and effectively manage these risks.
b) Continuously reviewing the business policies and procedures of the financial institution and monitoring their implementation in addition to recommending measures to be taken to meet the AML/CTF requirements and strengthening these measures as needed.
c) Continuous monitoring and examination of activities and transactions to ensure that their volume is consistent with the information that the financial institution has about the customer, its business activities, and the risks posed by that customer in order to detect activities that may include suspicious transactions in

addition to making use of such examinations in the preparation and update of AML/CTF monitoring methods approved.

d) Receiving reports on suspicious ML/TF transactions, taking the necessary measures to collect and analyze information about them, and documenting this in writing.
e) Reporting suspicious transactions to the SAFIU as soon as the suspicion is detected in accordance with the reporting procedures followed in addition to preparing a technical report on the suspicion case as stated in the Reporting of Suspicious Transactions Section.
f) Reporting any accounts, business relationships, or financial transactions related to the names included in the lists of the Security Council committees, Committee 2253/1989/1267 and Committee 1988, as well as the names included in the national list in implementation of Security Council Resolution No. (1373) to SAMA, as mentioned in Paragraph (8.15) under the Reporting of Suspicious Transactions Section.
g) Conducting frequent visits to the different departments and branches of the financial institution to ensure that AML/CTF requirements are met in addition to documenting such visits in writing.
h) Preparing and submitting on-site visit reports and periodic reports on activities carried out by the AML/CTF unit/function to the board of directors.
i) Preparing and approving a survey related to the AML/CTF internal controls approved by the financial institution when it enters into a business relationship with another financial institution.
j) Approving the internal controls survey, data collection forms, and any information related to combating ML/TF submitted to SAMA.
k) Participating in AML/CTF work committees.

9.4 The reports submitted to the board on the activities carried out by the AML/CTF unit/function shall not be limited to statistical data only; they shall also include the identified obstacles and challenges facing the financial institution when implementing the AML/CTF requirements along with the necessary recommendations to improve performance and effectiveness.

Section 10: Independent Audit Function

In order for the financial institution to ensure the adequacy and appropriateness of the risk-based approach, the financial institution shall have the AML/CTF internal controls tested by an independent party to ensure that they are adequate to ML/TF risks and implemented effectively. However, the internal or external auditors involved shall have sufficient experience to conduct a risk-based test of the effectiveness of implementing the AML/CTF policies and procedures approved by the financial institution.

Article (14/1) of the Implementing Regulations of the Anti-Money Laundering Law and Article (18) of the Implementing Regulations of the Law on Combating Terrorism Crimes and Financing state the obligations of the financial institution that include setting up an independent audit mechanism to test the effectiveness and adequacy of the AML/CTF policies, procedures and controls.

10.1 The financial institution shall put in place appropriate arrangements for the independent audit function, including providing sufficient resources to test compliance with the AML/CTF requirements and ensuring that the independent audit employees are qualified and have the necessary professional competence and capabilities to examine the compliance of all units in the financial institution with the AML/CTF requirements.

10.2 The auditor in the financial institution shall work independently of the AML/CTF function, and the financial institution shall ensure that the independent auditor is not involved in any of the functions or measures audited.

10.3 The independent auditor shall conduct an independent test of the appropriateness, adequacy and effectiveness of the AML/CTF compliance program and procedures at the level of the financial institution, document the audit results and send them to the board of directors to take the proper actions.

10.4 The independent auditor shall conduct independent tests of the AML/CTF controls, policies, and procedures and their adequacy for the risks identified.

10.5 When testing the appropriateness, adequacy and effectiveness of the AML/CTF compliance program and procedures, the independent auditor's work shall be based on ML/TF risks and focus on the risk areas that are more likely than others to be exploited in carrying out ML/TF transactions.

10.6 When necessary, the financial institution should consider including the auditing of the appropriateness, adequacy and effectiveness of the AML/CTF compliance function within the scope of the external auditor's work.

10.7 The senior management should take adequate measures to ensure that any weaknesses or deficiencies discovered as a result of the independent audit are addressed.

Section 11: AML/CTF Training

The financial institution should allocate sufficient budget for training the senior management and employees to achieve the required efficiency in combating ML/TF. The training needs to be inspired by real experiences and should include the updates and new methods used in ML/TF transactions and the internal controls of the financial institution. The responsibility for determining the appropriate level and type of training rests with the financial institution as it has to ensure the ability of its employees to apply the risk-based approach.

Article (14/1) of the Implementing Regulations of the Anti-Money Laundering Law and Article (18) of the Implementing Regulations of the Law on Combating Terrorism Crimes and Financing state the obligations of the financial institution including providing ongoing employee training programs in the field of AML/CTF.

11.1 The financial institution should organize ongoing training programs for all employees to acquaint them with the regulations, instructions and updates in the field of AML/CTF in a way that enhances the efficiency

of employees to identify these transactions and their typologies and know how to deal with them. These programs shall enable the employees to achieve a degree of knowledge sufficient to effectively reduce the occurrence of such crimes and combat them. In this regard, the financial institution should allocate sufficient budget to provide AML/CTF training.

11.2 The financial institution should provide appropriate training to its employees, taking into account the level of their position and nature of work. The training programs should include the various position levels in the financial institution, including members of the board of directors and its committees, managers, and executives. In addition, the following shall be observed:

a) Training and education about the importance of AML/CTF policies and measures shall be provided for all current employees and new employees before they start work. Such training must be repeated to ensure that employees are continuously reminded of their responsibilities and informed of the updates and developments in this regard.
b) Providing more comprehensive and detailed training for employees responsible for implementing due diligence, in line with the risks to which the financial institution is exposed.
c) Specialized and adequate AML/CTF training should be provided for the AML/CTF compliance function employees as well as the independent audit function employees.
d) All employees, directors and board members of the financial institution should be made aware of their responsibilities and duties as well as the penalties that may be imposed in case of failure to comply with the relevant requirements, as stated in the Anti-Money Laundering Law, the Law on Combating Terrorism Crimes and Financing, their Implementing Regulations, and the instructions issued by SAMA and the authorities concerned.

11.3 When seeking assistance from specialized institutes to provide training, the financial institution should take the following measures:

a) Verifying the suitability of the training offered for the AML/CTF requirements.
b) Ensuring that the training takes into account the nature of activities and the risks to which the financial institution is exposed.
c) Verifying the academic and work history of the trainer.
d) Polling the opinions of trainees on the suitability of the training materials and the style, experience and capabilities of the trainer in addition to analyzing the survey results after each training program to benefit from the trainees' observations.

11.4 The financial institution should conduct the necessary tests to assess the employees' knowledge of the AML/CTF requirements and the quality of training provided in this regard, provided that such assessment is carried out periodically (at least annually), taking into account the relevant modern requirements.

11.5 The financial institution shall keep records that include documents of the AML/CTF training provided, attendance data, and the date of training.

Section12: Recruitment and Following-up Criteria

The financial institution shall implement effective internal control systems that ensure the integrity of employees and reduce the risk of their involvement or collusion with criminals in order to ensure integrity and professional criteria among its employees.

Article (14/1) of the Implementing Regulations of the Anti-Money Laundering Law and Article (18) of the Implementing Regulations of the Law on Combating Terrorism Crime and Financing set forth the obligations of the financial institution, which include developing adequate screening procedures to ensure high standards when hiring employees.

12.1 The financial institution shall develop and implement an appropriate process for background checks for qualified candidates when hiring employees to ensure high efficiency standards.

12.2 The financial institution should verify the records of the board members, occupants of leadership positions, or employees to ensure that they have

no criminal background breaching honor or integrity, whether in Saudi Arabia, the country of nationality, or the country where they have previously worked.

12.3 The financial institution shall maintain the background verification procedures applied as stated in Paragraphs (12.1) and (12.2) and submit them to SAMA upon request.

12.4 The financial institution should comply with the provisions stated in the Requirements for Appointments to Senior Positions in Financial Institutions Supervised by SAMA.

12.5 The financial institution should study its need for a job rotation policy to reduce the risk of employees circumventing internal controls.

12.6 The financial institution should ensure that employees use their leave days regularly (at least once a year) and/or according to internal policies approved by the financial institution. It should also ensure that employees do not work during leave days.

Section 13: Correspondence Relationship[5]

Before entering into a correspondence relationship, the financial institution should collect sufficient information about the correspondent institution to obtain a full understanding of the nature of its work and learn about its reputation, the level of supervision applied to it, and the extent to which it applies the AML/CTF requirements.

Article (9) of the Anti-Money Laundering Law and Article (68) of the Law on Combating Terrorism Crime and Financing set forth the obligations that must be fulfilled by the financial institution before entering into a correspondence relationship.

13.1 Before entering into a correspondence relationship, the financial institution shall take sufficient measures to mitigate risks. These measures may include the following:

[5]Financial institutions must comply with the Correspondence Relationship Section in addition to the requirements of Rule (300-2-5) regarding non-resident commercial banks in the Rules Governing the Opening of Bank Accounts

a) Collecting sufficient information about the correspondent institution to fully understand the nature of its work, the supervision applied to it and the risks to which it is exposed as well as evaluate its reputation based on the information available to the financial institution. This may include:
   - The geographical areas in which the correspondent institution provides its services, taking into account those areas with shortcomings in the application of the AML/CTF requirements, as mentioned in Paragraph (4.7) under the Enhanced Due Diligence Section.
   - Ownership structure of the correspondent financial institution, taking into account the case of correspondent institutions with a complex organizational structure as the financial institution should implement the measures mentioned in Paragraph (4.6) under the Enhanced Due Diligence Section.
   - Services and products provided by correspondent institution, taking into account the products and services that may involve high risk from the perspective of ML/TF.
   - Customers of the correspondent institution, taking into account the information available on customers that pose high risks due to their activities or characteristics when a large part of the correspondent institution's business income depends on these customers.
   - The supervisory authority of the correspondent institution, taking into account that the correspondent institution must be supervised by the central bank or a similar regulatory body as well as an internationally recognized regulatory environment and its compliance with the FATF Recommendations.

b) Verifying the extent to which the correspondent institution is subject to an investigation or control procedure related to ML/TF.

c) Evaluating the internal policies, controls and procedures to mitigate risks that are adopted by the correspondent institution to combat ML/TF by preparing a questionnaire that covers basic

AML/CTF requirements and assesses the effectiveness of measures.

13.2 The financial institution should clearly understand the responsibilities of each party in the correspondence relationship from an AML/CTF perspective.

13.3 The financial institution should apply appropriate control measures as indicated under the Monitoring of Transactions and Activities Section, including continuous control measures for correspondence accounts to detect any unusual activity or behavior in the correspondence relationship.

13.4 The financial institution should be sufficiently satisfied that the correspondent institution does not allow its accounts to be used by a shell bank. The financial institution shall refrain from entering into -or continuing- a correspondence relationship with a shell bank or with a financial institution outside Saudi Arabia that allows its accounts to be used by a shell bank.

13.5 Approval of the senior management should be obtained before establishing new correspondence relationships, provided that the approval includes taking the measures mentioned in Paragraph (13.1) under the Correspondence Relationship Section and obtaining recommendations from the officer responsible for the AML/CTF compliance function.

Section 14: Wire Transfer

When carrying out cross-border or domestic wire transfers in any currency, including serial and coverage payments, that are received, sent or processed by a financial institution in Saudi Arabia, the financial institution should obtain information of the wire transfer originator and beneficiary, including cases in which a credit card, debit card, prepaid card, mobile phone, or any other similar digital prepaid or postpaid device is used.

Article (10) of the Anti-Money Laundering Law and Article (68) of the Law on Combating Terrorism Crimes and Financing state the obligations of the financial institution when conducting cross-border and domestic wire transfers in any currency, including serial payments and coverage payments, that are received, sent or processed by a financial institution in Saudi Arabia.

14.1 Before processing a wire transfer, the financial institution should obtain information about the wire transfer originator and beneficiary, keep that information with each wire transfer, and verify that information. Such information shall at least include the following:

a) Full name of the wire transfer originator.
b) The originator's account number used for conducting the transaction, and if there was no account, a transfer number must be included to allow the transaction to be tracked.
c) The originator's address, ID number, customer identification number, or place and date of birth.
d) Full name of the wire transfer beneficiary.
e) The beneficiary's account number used for conducting the transaction, and if there was no account, a transfer number must be included to allow the transaction to be tracked.
f) The purpose of the wire transfer and the relationship between the originator and the beneficiary.

14.2 Before executing a wire transfer, the financial institution should obtain a declaration from the customer stating his knowledge that Saudi Arabia's laws prohibit the transfer of funds without the customer's knowledge of the beneficiary (transferee), without a legal relationship with the beneficiary, or without a legitimate purpose.

14.3 In cases where several individual cross-border wire transfers are combined from a single originator in a combined transfer to beneficiaries, the financial institution responsible for originating the transfer shall verify the information attached, including the originator's previously verified information as well as the beneficiary's full information, as stated in Paragraph (14.1). This is to allow tracking of the transfer within

the country in which the beneficiary is located in addition to the originator's account number and the reference number of the transfer.

14.4 In the case of a domestic wire transfer and when the financial institution originating the transfer was able -through other means- to provide all information about the wire transfer originator and beneficiary to the financial institution receiving the transfer or the competent authorities, the financial institution is exempt from adding information to each wire transfer. The financial institution originating the transfer may include an account number or a transfer number that allows linking the transaction with relevant information about the wire transfer originator or beneficiary. Furthermore, the financial institution originating the transfer should provide all information about the wire transfer originator and beneficiary within three working days starting from the date of receiving a request for that information from the financial institution or the competent authority.

14.5 The financial institution and the intermediary financial institution receiving a wire transfer from outside Saudi Arabia should prepare and implement policies, procedures and controls for the following purpose:

a) To identify wire transfers that lack the required information regarding the originator or beneficiary.
b) To determine cases of executing, rejecting or suspending a wire transfer due to lack of required information related to the originator or beneficiary based on risks.
c) To conduct adequate monitoring based on risks that may include restricting or terminating the business relationship.

14.6 The financial institution receiving a wire transfer from outside Saudi Arabia shall take reasonable measures to identify transfers that lack the required information relating to the originator or beneficiary. These measures may include follow-up procedures after implementation or during implementation, as applicable. In the event of not having the identity of the beneficiary previously verified, the financial institution

receiving a wire transfer shall verify the beneficiary's identity and keep this information as stated under the Record Keeping Section.

14.7 The confidentiality requirements stated under domestic laws do not preclude the financial institution from exchanging information with another local or foreign financial institution that is processing any part of the transaction as required under the Wire Transfer Section.

14.8 The scope of the Wire Transfer Section requirements does not include the following:

a) Transfers that result from a transaction carried out using a credit card, debit card, prepaid card, mobile phone, or any other similar digital prepaid or postpaid device only for the purchase of goods or services, provided that the credit or debit or prepaid card number accompanies the transfer resulting from the transaction.
b) Transfers that constitute a transfer or settlement between two financial institutions when the originator and the beneficiary are financial institutions acting on their own behalf.

14.9 In the event that the financial institution is unable to comply with the requirements of Paragraph (14.1), it should not perform the wire transfer.

14.10 The financial institution and the intermediary financial institution should not accept executing a cross-border wire transfer in any currency for charitable purposes[6] regardless of the source of funds or the beneficiary, taking into account what is stated in Paragraph (14.7).

14.11 The financial institution and the intermediary financial institution receiving wire transfers from outside Saudi Arabia shall not accept these transfers in any currency for charitable purposes, regardless of the source of funds or the beneficiary, taking into account what is mentioned in Paragraph (14.7).

[6]In the event that a financial institution receives an approval from SAMA indicating that some parties are allowed to transfer gifts, subsidies, or donations to a beneficiary, whether it be a legal or natural person, in accordance with certain conditions, the financial institution must act according to that approval

14.12 Business of the intermediary financial institution providing wire transfer services related to transactions executed through the financial institution, with which it has a contract, should be subject to supervision and control.

14.13 The information exchanged with a correspondent financial institution or an intermediary financial institution providing wire transfer services must only be used for authorized purposes subject to the terms and conditions of confidentiality and should never be used for any other purposes.

14.14 The financial institution and the intermediary financial institution shall not receive a wire transfer from outside Saudi Arabia to a beneficiary in a financial institution abroad if the wire transfer is in a currency other than the Saudi riyal.

14.15 The financial institution may receive a wire transfer from outside Saudi Arabia to a beneficiary in a financial institution abroad only when the wire transfer is in the Saudi riyal currency, taking into consideration what is stated in Paragraphs (14.1), (14.5) and (14.8).

14.16 The financial institution and intermediary financial institution receiving a wire transfer in the Saudi riyal currency from outside Saudi Arabia to a beneficiary in a financial institution abroad shall clearly detail the purpose of the transfer.

[5] In the event that a financial institution receives an approval from SAMA indicating that some parties are allowed to transfer gifts, subsidies, or donations to a beneficiary, whether it be a legal or natural person, in accordance with certain conditions, the financial institution must act according to that approval.

بسم الله الرحمن الرحيم

مؤسسة النقد العربي السعودي

المركز الرئيسي

إدارة مكافحة غسل الأموال وتمويل الإرهاب

المرفقات (٤٨) ورقة لدليل مكافحة غسل الأموال وتمويل الإرهاب.

"تعميم"

سعادة /

المحترم

بعد التحية:

الموضوع: دليل مكافحة غسل الأموال وتمويل الإرهاب.

انطلاقاً من دور المؤسسة الإشرافي والرقابي، وحرصاً منها على حماية القطاع المالي وسمعته من إساءة الاستغلال في عمليات غسل أموال أو تمويل إرهاب وبناء على الصلاحيات الممنوحة للمؤسسة بموجب المادة الرابعة والعشرون من نظام مكافحة غسل الأموال الصادر بالمرسوم الملكي الكريم رقم (م/٢٠) وتاريخ ١٤٣٩/٠٢/٠٥هـ، والمادة الثانية والثمانون من نظام مكافحة جرائم الإرهاب وتمويله الصادر بالمرسوم الملكي الكريم رقم م/٢١ وتاريخ ١٤٣٩/٠٢/١٢هـ.

وإشارة إلى قواعد مكافحة غسل الأموال وتمويل الإرهاب للبنوك ومحلات الصرافة وفروع البنوك الأجنبية (التحديث الثالث) الصادرة بموجب التعميم رقم ١٨١٤٧/م أ ت/٩٢٠١ وتاريخ ١٤٣٣/٠٤/٠٤هـ، وقواعد مكافحة غسل الأموال وتمويل الإرهاب لشركات التمويل (التحديث الأول) الصادرة بموجب التعميم رقم ١٨٥١٦/م أ ت/٩٢٥٣ وتاريخ ١٤٣٣/٠٤/٠٦هـ، وقواعد مكافحة غسل الأموال وتمويل الإرهاب لشركات التأمين وإعادة التأمين وشركات المهن الحرة (التحديث الأول) الصادرة بموجب التعميم رقم ت.ع.م/٢٠١٢٠٢/٢٢ وتاريخ ١٤٣٣/٠٤/٠٧هـ.

مرافق دليل مكافحة غسل الأموال وتمويل الإرهاب، المتضمن الحد الأدنى من متطلبات نظام مكافحة غسل الأموال ونظام مكافحة جرائم الإرهاب وتمويله الذي ينبغي على المؤسسة المالية الالتزام به، ليحل الدليل محل القواعد المشار إليها أعلاه. وعلى المؤسسة المالية عرض الدليل على مجلس الإدارة وتحديد مسؤولياته ومسؤوليات الإدارة العليا ومسؤوليات الموظفين حيال الدليل، وتوعية منسوبي المؤسسة المالية حيال التزاماتهم فيما تضمنه الدليل.

وتقبلوا خالص تحياتي

أحمد بن عبد الكريم الخليفي

المحافظ

نطاق التوزيع:

- شركات التمويل العاملة في المملكة.
- البنوك والمصارف العاملة في المملكة.
- شركات ومؤسسات الصرافة العاملة في المملكة.
- شركات المدفوعات ونظم المدفوعات العاملة في المملكة.
- شركات التأمين وإعادة التأمين وشركات المهن الحرة العاملة في المملكة.

السيف

ص.ب ٢٩٩٢ - الرياض ١١١٦٩ - هاتف ٠١١ ٤٦٣٣٠٠٠