Anti-Money Laundering and Terrorism Financing Policy for Bank of Jordan Group
# Table of Contents

1. Introduction 3
2. Legal Framework for the Implementation of the Anti-Money Laundering and Terrorism Financing Policy 4
3. Definition of Money Laundering, Terrorism Financing and Acts of Terrorism 5
4. Stages of Money Laundering 6
5. Crimes Related to Money Laundering and Acts of Terrorism 7
6. Know Your Customer Policy 8
   - Customer Acceptance 9
   - Classifying Customers According to Degree of Risk 13
   - Customer Diagnosis and Analysis 16
   - Continuous Monitoring of Accounts and their Operations 18
7. Know Your Employee Policy 19
8. Principles to be Considered in Carrying out Credit and Debit Operations 21
9. Requirements for Dealing with Foreign Banks 23
10. Mechanism of Identifying and Reporting Suspicious Transactions 24
11. Reporting Channels 25
12. Duties and Responsibilities of the Board of Directors 26
13. Duties and Responsibilities of the Senior Executive Management 27
14. Duties and Responsibilities of the Anti-Money Laundering and Terrorism Financing Unit 27
15. The Duties and Responsibilities of the Liaison Officer 28
16. Duties and Responsibilities of the Money Laundering Reporting Officer (MLRO) 29
17. Reviewing and Approving the Anti-Money Laundering and Terrorism Financing Policy 31
18. Training and Qualifying Employees 32
19. Updating Data 32
20. Documents and Record Keeping 33
21. Security Council Resolutions 33
22. Methodology for Self-Assessment of the Risks of Money Laundering and Terrorism Financing at the Level of the Group 34
23. General Rules 36
24. Definitions 38
25. Particular Annexes 42
1. **Introduction**

The phenomenon of money-laundering and Terrorism Financing has recently become one of the most concerning criminal phenomena in the world due to it being linked with organized crime and particularly drug dealing as the perpetrators of these crimes have benefited from the scale of successive developments in the field of information technology, communication and means of transportation. This is in addition to the significant growth in trading activities which resulted in huge flow of goods and services between different countries.

The operations of Terrorism Financing and money-laundering are two sides of the same coin and are closely bound together as studies have shown that most terrorism acts are fund from money-laundering.

Money launderers have taken advantage of the merger in international money markets and the technical development in banking and finance systems, which have become the main channels for them to move and transfer the to-be-laundered money anywhere in the world and therefore, hiding its illegal source.

As such, and considering that commercial banks are deemed a place for most money-laundering crimes and Terrorism Financing, the role of the banks in monitoring Suspicious Transactions performed by money launderers is one of the most significant practical methods to Control and counter Money Laundering. This requires the presence of clear procedures and policies that aim to protect the bank's reputation and avoid operational risks that may arise as a result of the bank being used as a channel for Money Laundering. Moreover, local regulations and instructions of the regulatory bodies that have been issued in this regard represent the general framework which must be compelled with and the necessary measures for its implementation must be taken, this is in addition to the worldwide requirements and international laws which set conditions on internal and foreign bank transactions as well as on the relationships with correspondent banks.

Furthermore, the efforts the bank places in implementing these procedures to ensure that the money resulting from suspicious operations are not conducted through the banking and finance system of Bank of Jordan will have a positive effect on the bank's local and international image and in the bank avoiding any obstacles in managing its banking and financial transactions.
2. Legal Framework for the Implementation of the Anti-Money Laundering and Terrorism Financing Policy

First: Legal Framework

1. Operating branches in the Kingdom:

1.1 Local laws:

1.1.2 The Banking Law No. (28) for the Year (2000) Articles (93) and (99/B).
1.1.4 The Amended Law for Anti-Terrorism for the Year (2014) and is read with Law No. (55) for the Year (2006).

1.2 Instructions/ curriculars of the Jordanian Central Bank of Jordan

1.2.1 Instructions on Dealing with Customers with Fairness and Transparency No. (56/2012) date 31/10/2012, and the Amending Instructions No. (57) for the Year (2013).
1.2.2 Anti-Money Laundering and Terrorism Financing for Licensed Banks (14/2018).

1.3 Instructions issued by other monitory authorities pursuant to local laws:

1.3.1 Instructions No. (1) for the Year (2015) on forms and methods for reporting suspicious operations related to Money Laundering or Terrorism Financing, issued by the head of Anti-Money Laundering and Terrorism Financing Unit pursuant to the provisions of the laws and regulations.
1.3.2 Instructions No. (3) for the Year (2018) for implementing the responsibilities stated in the Securities Council’s resolution No. (1373) (2001) and other related resolutions issued by the National Committee for Anti-Money Laundering and Terrorism Financing pursuant to Paragraph (C) of Article (37) of Anti-Money Laundering and Terrorism Financing No. (46) for the Year (2007) and its Amendments.

2. Subsidiaries of Bank of Jordan that are operating inside the Kingdom if subject to regulatory bodies other than the Central Bank, and operating branches outside the Kingdom.

2.1 Instructions in this policy are applied to all subsidiaries of Bank of Jordan operating inside the Kingdom if said subsidiaries are subject to regulatory bodies other than the Central Bank of Jordan, and to the extent it is consistent with the instructions issued by the regulatory bodies which oversee these subsidiaries.
2.2 Instructions in this policy are applied to branches/companies which are subsidiaries of the Bank that are operating outside the Kingdom and to the extent permitted by the laws, regulations and instructions issue by the regulator in the hosting country in which these subsidiary branches/companies operate.

2.3 In case of discrepancy between the requirements of Anti-Money Laundering and Terrorism Financing in the hosting country and the mother country, the stricter requirements are to be applied, and the Bank is obliged to notify the Central Bank of any obstacles or restrictions that may challenge or prevent the application of these instructions.

Second: Scope of application
This policy is considered the master policy for all subjects of Anti-Money Laundering and Terrorism Financing to all members of the Bank of Jordan Group (foreign branches and subsidiaries), and represents the main guidelines to be complied with, all with consideration to all laws and instructions of the hosting country which the foreign branch or subsidiary companies are located. In case of any discrepancy between the provisions of this policy and the laws and instructions of the hosting country of the foreign branch or subsidiaries, the stricter instructions shall be applied.

In the event there is discrepancy between this policy and the laws regulating subjects related to Anti-Money Laundering and Terrorism Financing, foreign branches and subsidiaries have the right to place policies that derive from this policy and that comply with the laws of the hosting country, and these policies shall be deemed pursuant to this provision, issued from the Board of Directors.

3. Definition of Money Laundering, Terrorism Financing and Acts of Terrorism

- **Money Laundering** is defined as every criminal act that aims to conceal and hide the true source of money which was acquired illegally by conducting a series of successive procedures which eventually lead to the appearance that the money is a result of legitimate business activities.

- **Terrorism Financing** is defined as carrying out any banking operation by depositing money at any bank or Financial Institution that conducts banking operations, or transferring money to any party for the purpose of providing or making available the said money to an individual, group or organization with the intent of using the money to conduct terrorist acts in the aim of disturbing the public order or endangering the safety and security of the society.

- **Act of Terrorism** is defined as every intentional act, threat, or omission, regardless of its motives, purposes, or means, that is carried out for a crime whether by an individual or a group, that endangers the safety and security of society or causes disorder if such act causes disturbance of public order or castes terror among people or endangers their lives
or harms the environment or public facilities and properties, private properties, international facilities, diplomatic missions, causes occupation or seizing of any of them or endangers national or Economic Resources, forces a national or legal authority or an international organization or a regional organization to perform an act or to abstain from performing an act, or obstructs the implementation of the constitution, laws or regulations.

- **Hence, the Money Laundering procedure includes:**
  1. Utilizing or possessing illegal money.
  2. Utilizing the illegal money by any means through a series of bank operations or purchasing movable and immovable assets.
  3. Providing incorrect or false information regarding the source of money to hide and conceal the actual source of the illegal money.

- **Why money is laundered**
  The retention of illegal money by their owners without a logical justification for how they obtained them leads to the discovery of their crime. Hence, the seek to conduct operations and activities as if these operations and activities are the actual source of the money in their possession.

4. **Stages of Money Laundering**

   Operations conducted for the purpose of laundering money are considered complex and diverse operations. These operations may not include cash operations, however, they mainly go through three main stages:

   1. **Placement**
      In this stage, money derived from crime or illegal operations are invested or inserted into the financial system through cash deposits or the purchase of various financial instruments. This stage is considered the most difficult stage for money launderers as the dirty money is exposed to the discovery of its illegal source, this stage is not necessarily carried out by the real owner of the dirty money, he may use the account of another customer as an intermediary to serve the actual owners of the money for a commission in return.

   2. **Layering**
      In this stage, the connection between the money and its illegal source is concealed and/or camouflaged by performing a series of complex and successive operations of purchasing, selling, transferring and any other financial or non-financial activities that are difficult to track.
3. **Integration**

During this stage the laundered money is integrated into the economy so that it becomes difficult to distinguish it from money resulting from legitimate sources (showing the money within the legitimate economic system).

5. **Crimes Related to Money Laundering and Acts of Terrorism**

   **A. Different crimes may be a source of dirty money which owners seek to hide and conceal from its actual source, some of which are:**

   1. Illegal trade in materials, goods and services that are not permitted locally or internationally, the most important of which are planting, manufacturing, and trading drugs and psychotropic substances.
   2. Cross-border smuggling activities for legitimate imported goods, in the aim of evading the payment of fees and custom duties imposed on importation, as well as smuggling illegal goods such as weapons.
   3. Embezzlement, theft, and fraud crimes.
   4. Counterfeiting and forgery of currencies, gold, precious metals.
   5. Theft of antiquities and valuables, as well as armed robbery.
   7. Political and managerial corruption, as well as bribery through illegitimate utilization of public services for personal benefit.
   8. Tax evasion.
   10. Kidnapping, piracy, and terrorism.
   11. Harming the environment.
   12. Prostitution and gambling.

   **B. Subject to the provisions of the Penal Law or any other law, the following acts are deemed as acts of terrorism and are banned:**

   1. Performing directly or indirectly any means of providing, collecting or procuring money with the intention of utilizing the money to commit an act of terrorism or to fund terrorists, regardless if the act was committed or not, is intended to be committed or was committed inside or outside the Kingdom or is related to its citizens or their interests.
   2. Performing actions that expose the Kingdom to the risk of hostile acts, disturbs its relationships with foreign countries, or exposes Jordanians to the risk of reprisals against themselves or their money.
   3. Committing or attempting to commit a terrorist act through another person or participating, aiding, organizing or directing others in committing a terrorist act, or having knowledge of a person or organization’s intention to commit or encourage or contribute in a terrorist act with people working for a common purpose, regardless of whether this contribution or participation is deliberate or intended to reinforce the performance of the
terrorist act, or knowledge of a person’s intention to commit a terrorist act, and regardless of the means and of his own free will, whether directly or indirectly and whether the terrorist act took place or not.

4. Committing or attempting to commit a terrorist act through an organization, body, association, group, or cell consisting of two or more persons, whether the act was committed or not, or participating or contributing or aiding or organizing others in performing a terrorist act with people working for a common purpose so that this contribution is deliberate and is in the aim of encouraging the performance of the terrorist act, or with the knowledge or intent or determination of committing it, by any means and directly or indirectly.

5. Joining or attempting to join any armed groups or Terrorist Organizations or recruiting or attempting to recruit people or training them for the said purpose, whether inside or outside the Kingdom.

6. Establishing or joining an association, group or organization with the intent to commit terrorist acts in the Kingdom, or against its citizens or their benefits outside the Kingdom.

7. Utilizing any information system, informational network, or any publishing or media means, or creating a website to ease the performance of terrorist acts or to support a group, association, or organization that performs terrorist acts, or promotes their ideas or funds them, or performing any act that may expose Jordanians or their assets to the risk of hostile or reprisal actions against them.

8. Possessing, manufacturing, importing, exporting, carrying, or selling any explosive, toxic, flammable, or chemical materials or any other similar materials, or dealing with weapons or ammunition for the purpose of using them to perform terrorist acts or in an unlawful manner.

9. Assaulting the life, liberty or freedom of the king or queen or the crown prince or any guardian to the throne.

10. Any act carried out with the intention of provoking an armed rebellion against the existing authorities established under the constitution, or preventing the authorities from exercising their functions which are derived from the constitution, or amending the constitution of the country in unlawful methods.

11. Forming a gang with the intent to rob passers-by, attack people or assets, or commit any act of robbery.

6. **Know Your Customer Policy**

The pattern and form of Suspicious Transactions cannot be the sole preventative instrument against Suspicious Transactions, it cannot be relied on without knowing the customer and the nature of the customer’s activities, rather they are signals which do not necessarily mean that the transaction involves Money Laundering or Terrorist Financing. It is necessary to link the pattern and form of Suspicious Transactions with additional information relating to the customer’s personality, nationality, place of residency, type and size of activities he engages in, in addition to other information that provide a complete understanding of the nature and type of transactions and relationships related to the customer and his activities.
• **Key elements of customer recognition policies (customer due diligence):**

  Customer due diligence means knowing the customer's identity, legal status, activity, the purpose of the business relationship between the customer and the actual beneficiary (if any), and in the event there is any person acting on behalf of the customer comparing the name of the customer and the actual beneficiary and the authorized signatory (if any) with the names of persons and entities listed on the banned list issued pursuant to the resolutions of the Security Council. This is in addition to verifying the identification data from unbiased and trusted sources, following up with transactions that are performed within a continuous relationship by any means specified pursuant to the relevant legislations, as well as knowing the nature and purpose of the future relationship between the bank and the customer, and verifying the sources of money for transactions that are performed within the frame of the Banking Relationship.

  The following basic elements constitute the main and most helpful part in limiting Money Laundering operations and Terrorist Financing, in addition to being the backbone of the bank's operational risk management:

  1. Customer acceptance.
  2. Classifying customers according to degree of risk.
  4. Continuous monitoring of accounts that are of a high risk.

**First: Customer Acceptance**

The customer acceptance policy is considered the first protective wall to avoid the risks that may arise a result of dealing with customers. At this stage, it is possible to refuse dealing with the customer or to estimate the level of risk related to the customer depending on the type of many elements some of which are; economic activity, nationality, political position, public service. The following policies are related to accepting dealing with the customer:

1. **Procedures for customer identification and verification**

   1.1 Identification procedures for identifying a customer who is a natural person:

      1.1.1 The identification data must include the customer's full name, date and place of birth, national number, as well as all information related to the identification document for Jordanians. For non-Jordanians, the passport number, personal number, nationality, permanent residency address, annual residency permit issued by the Ministry of Interior or valid work permit if the customer is an expat, phone number, work address, type of activity, purpose of business relationship and its nature, name of those authorized to manage the account, their nationalities, and any other information the Bank deems necessary.

      1.1.2 As for persons lacking legal capacity such as minors, documents relating to the legal representatives handling their accounts must be obtained.
1.1.3 In the event a person deals with Bank of Jordan on behalf of a customer, it is necessary to ensure that a valid power of attorney or a bank approved authorization is presented, with the necessity to obtain approval of the document from the legal department as well maintaining the power of attorney or the authorization or a certified copy of them, in addition to the importance of identifying the identity of the agent as per the identification procedures mentioned in paragraph (1.1).

1.1.4 Verification of the validity of the natural person's identity is conducted. This is conducted by referring to the Civil Status Department for Jordanians, and by obtaining a copy of a valid passport as well as any other documents that are proof of identity for non-Jordanians all signed by the competent employee stating that it is a true copy, with the customer signing a pledge to provide the bank with a copy of the passport in the event it is renewed. Additionally, proof of employment and all other sources of income are to be obtained (such as an original copy of the employment contract or a salary slip) as well as verification of the customer's addresses by obtaining a copy of the lease agreement or invoices for public services.

1.2 Identification procedures for identifying a legal entity or arrangement:

1.2.1 Identification data should include the name of the legal entity or arrangement, legal form, names of shareholders or owners and their addresses, ownership shares, authorized signatories, address of the headquarter, type of activity, capital, date of registration and its number, tax number, the national number of the legal entity, names of people authorized to deal with the account and their nationalities, phone numbers and the purpose of the business relationship, so as the Bank has full knowledge of the ownership structure and the names of the people concerned that fulfill senior management positions in the legal entity or arrangement. This is in addition to the provisions governing the decisions that are binding upon the legal entity, in addition to verifying the nature of the customer and the ownership structure, guardian council in regards to Legal Arrangements, and any other information the Bank deems necessary, all must be kept updated.

1.2.2 Verification of the existence of the legal entity, names of owners or shareholders, names of authorized signatories, through the necessary documents and the information they contain, with referral to the website of the Companies Control Department and Ministry of Industry, Trade and Supply. For example, memorandum and articles of association for the legal entity, certificates issued by the Ministry of Industry, Trade and Supply, Amman Chamber of Commerce and Amman Chamber of Industry. Verification should also be conducted by verifying the customer's addresses by visiting the headquarters of the customer, profession license, in addition to obtaining a formal certificate duly issued by the competent authorities if the legal entity is registered outside the Kingdom.

1.2.3 Obtaining the documents that contain the existence of an authorization from the legal entity or arrangement for normal persons who are authorized to deal with the account, in addition to the importance of verifying the identity of the
authorized person as per the identification procedures and ensuring there are no legal impediments to dealing with the said people and obtaining their signatures.

1.2.4 Public shareholding companies are excluded from providing the data related to the names of the shareholders, their addresses and their shares, it is sufficient to request data relating to shareholders owning more than (10%) of the company’s share capital along with obtaining an undertaking from the authorized signatories to provide the Bank with the data of any shareholder whose shareholding falls within the said percentage.

1.3 Identification procedures for identifying a nonprofit organization

1.3.1 Identification data should include the name of the nonprofit organization, the legal form, the national number of the organization (if any), headquarter address, type of activity, date of establishment, names of those authorized to deal with the account and their nationalities, phone numbers, purpose of the dealing, sources of finance and income, and any other information the Bank deems necessary to obtain.

1.3.2 Verification that the nonprofit organization is legally existing, verification is conducted through formal documents and the information they contain, such as certificates issued by the Ministry of Social Development or any other competent authority.

1.3.3 Obtaining documents indicating an authorization from the nonprofit organization for the natural persons who are authorized in dealing with the account in addition to the importance of identifying the authorized person as per the procedures for identifying customers.

1.3.4 Verifying the data provided by the customer through bias and trusted sources, including contacting the competent authorities that issue formal documents proving that these documents are true such as the Ministry of Social Development, and verifying if they are authorized to practice their activities inside the Kingdom and/or accept donations and funds from internal or foreign sources, as well as referring to the website for the registry of nonprofit organization and verifying the customer’s address by visiting the headquarters of the customer and the profession license.

1.4 Identification procedures for identifying a foreign, unregistered company that is not permitted to operate inside the Kingdom:

1.4.1 Ensuring that such companies opening bank accounts and performing any transactions in the Kingdom comply with the laws and regulations in force, taking into consideration the nature of the transactions conducted through these accounts, while being provided with a legal opinion from the legal department in this regard.
2. **Policies related to customer acceptance.**

2.1 The necessity of referring to the approved Unified List relating to anti-terrorist financing and Money Laundering, as well as the lists issued by the Security Council prior to commencing or continuing a Banking Relationship. In the event there is an identical or similar name, the branch must contact the Anti-Money Laundering and Terrorism Financing Unit / Compliance Department to take the necessary action, and to halt the establishment of the Banking Relationship.

2.2 Referring to the list made by the Technical Committee deriving from the National Anti-Money Laundering and Terrorism Financing Committee prior to establishing the Banking Relationship to ensure that the customer's name is not listed, or its name is not similar or identical to a listed name within the list of Terrorist Persons or organizations, and the branch must therefore address the Anti-Money Laundering and Terrorism Finance Unit / Compliance Department to take the necessary actions and must halt the establishment of the Banking Relationship.

2.3 All information and data contained in the account opening application must be filled out based on the supporting original formal documents, while annotating that the original has been presented and viewed.

2.4 The branch must take all necessary procedures to validate the correctness of the data and information obtained from the customer through bias and trusted sources, including but not limited to, the database of the Civil Status Department to verify the data in the identity and requesting electricity or water bills, or a lease agreement to verify the address.

2.5 Obtaining a copy of all supporting documents relating to the nature of the activities of the customer, with the importance of keeping a copy of the documents, while annotating that the original has been presented and viewed must be written.

2.6 When opening correspondence accounts, a recommendation or authentication of the customer's signature and the required documents must be obtained as per the requirements for identifying the customer from banks or well-known Financial Institutions or through a Financial Institution that is a subsidiary to the same group, or certified or authenticated by the official bodies such as (foreign and Jordanian embassies and consulates). Furthermore, (correspondence accounts shall not be opened for people residing in the same country where the branch operates).

2.7 Verifying that the customer does not have any reservations on the deposit transactions conducted on his account by any other person, otherwise the customer must declare to the Bank the names of the people authorized to deposit.

2.8 Digital accounts are not permitted, nor establishing a Banking Relationship with anonymous persons or with fake identities or listed entities.

2.9 Leasing safe deposit boxes for non-customers of Bank of Jordan is not permitted, also the purpose of the lease and information of old customers must be updated in the event they wish to rent a safe deposit box.

2.10 Customer’s accounts with credit balances shall be deemed frozen (dormant accounts) if no deposit or withdrawal transactions are performed on the account without being able to infer the existence of the account holder through his other dealings with the Bank and
after exhausting all means of communication with the holder and after the expiry of the period specified under the relevant and applicable instructions in force.

2.11 Identities of the persons performing deposits should be obtained if performed by people other than those authorized to deposit, the identities must be filed in the database of the banking system by filling out the source of the money form which contains fields relating to (purpose of the deposit, source of the deposited money, relationship between the person performing the deposit and the account holder, type of document and its number, date of birth, the entity the depositor belongs to).

2.12 The Bank shall take all necessary procedures to verify the actual beneficiary by filling out the related clause in the cases that require so, and shall take the necessary procedures to identify the identity of the actual beneficiary as per the customer's risk profile, all in reliance on the data and information obtained from the official documents so that the Bank is fully convinced that the identity of the actual beneficiary is known.

2.13 The Bank shall take reasonable measures towards the actual beneficiary and the legal person to find out the ownership structure and the management in Control including identifying the natural person (or person) (if any). In the event it is not possible or there are any doubts towards identifying the identity of the natural person, the Bank must identify the natural person in Control of the legal entity through different means, otherwise the Bank must take reasonable measures to identify the natural person fulfilling a senior management position in the legal entity.

2.14 If the customer is a legal arrangement, the Bank must take into consideration the following when identifying the actual beneficiary:

2.14.1 Express Trusts: identifying the identity of the settlor, guardian or custodian (as the case may be) and the beneficiary for each natural person that exercises actual Control over the trust fund, including but not limited to (guardianship, custodies and agencies).

2.14.2 Other types of Legal Arrangements: identifying the identities of persons occupying positions equivalent or similar to those mentioned above, including but not limited to (company accounts and any accounts operating with mutual agreement between two parties in which a new identity will arise, such as joint accounts).

Second: Classifying Customer According to Degree of Risk

The purpose of classifying customers according to degree of risk when commencing a relationship with the Bank is to organize and increase the competence and efficiency of the Anti-Money Laundering and Terrorism Finance operations by determining the degree of care required prior to establishing the Banking Relationship.

Accordingly, the Bank has set the following principles and criteria for classifying customers:

1. **Classification degrees:**
   - High risk
   - Medium risk
   - Low risk

2. **Classification basis**
   - Classifying customer on the basis of risk is considered an aiding tool in determining the nature of the future relationship with the customer and the foundations and basis that need to be
followed in order to monitor and follow up with the transactions of the customer in a manner complying with the requirements of the regulatory bodies. In order to achieve the aforementioned, one can rely on the extent to which the banking transactions performed by the customer are in proportion to the nature of his activity and the amount of declared income. In addition to the complexity of the accounts opened at the Bank and the overlap between them, the movement rate, service channels, activities, products, and services provided to the customer. Nonetheless, it is difficult to lay and define certain foundations and basis to be applied on all customers.

As such, the following indicators have been determined and identified as a basis for classifying customers, to be reviewed and amended on an ongoing basis to be up-to-date with the latest available data that may lead to amendments of some of the provisions:

**First: High risk customers:**

High risk customers are those to whom the following indicators apply:

1.1 **Natural persons including the following:**

1.1.1 Politically exposed foreign persons: politicians who currently or previously occupied a senior public position in a foreign country, such as president, prime minister, judicial officials, military officials, members of political parties, high-level government positions, politicians, senior executive in foreign country owned companies, members of senior management i.e. managers, deputy manager, board of directors, or equivalent positions in international organizations. This also includes first-degree relatives as a minimum or their work partners or any person working on their behalf or have authorizations issued by them.

1.1.2 Politically exposed local persons: politicians who currently or previously occupied a senior public position in the Kingdom, such as prime minister, judicial officials, military officials, members of political parties, high-level government positions, politicians, senior executive in government owned companies, members of senior management i.e. managers, deputy manager, board of directors, or equivalent positions in international organizations, these people are classified as customers of high risk and this also includes first-degree relatives as a minimum or their work partners or any person working on their behalf or have authorizations issued by them.

1.1.3 People who engage in the following jobs:

- Owners of jewelry companies.
- Owners of currency exchange companies.
- Owners of weapon trading companies.

1.1.4 Persons not residing in the Kingdom regardless of their occupation locally or internationally.

1.1.5 Customers from high risk countries which are; countries listed on the FATF list as high risk countries regarding Money Laundering and
Terrorism Financing, or that have deficiencies in Anti-Money Laundering and Terrorism Financing measures which poses a threat to the global financial system, or the Kingdom has information that these countries pose a high risk regarding Money Laundering and terrorist financing in terms of countries that finance or that support terrorism, or in which there are Terrorist Organizations or agents who belong to any of the countries that are subject to international sanctions programs such as and without limitation; (UN, EU, OFAC).

1.2 **Legal entities including the following:**

1.2.1 **Economic activities**
- Travel and tourism companies.
- Insurance companies.
- Import and export companies.
- Goldsmithing companies.
- Fast food companies (especially if international brands).
- Hotels, coffee shops, night clubs, alcohol trading companies.
- Non-profit associations, companies, and entities.
- Currency exchange companies.
- Investment companies (real estate...).
- Real estate offices.

1.2.2 **Nationality:**
- All non-profit associations, companies, and entities regardless of the economic activity they practice.

1.2.3 **Business nature (main owner/ members of the board of directors/ shareholders holding (%10) or more shares/ general manager, the authorized signatory, the actual beneficiary)**
- If the customer is classified as a high risk customer, this risk is reflected on the risk classification of the company (high risk).

1.2.4 If any of the (main owner/ members of the board of directors/ shareholders holding (%10) or more shares/ general manager, the authorized signatory, the actual beneficiary) are politically exposed people whether local or foreign, this risk is reflected on the risk classification of the company.

1.2.5 **Charity associations/ nonprofit organizations.**

1.2.6 Nonoperating foreign companies.

**Second: Medium Risk Customers.**
- Each customer (natural/legal) who has any commercial activity, and who the abovementioned indicators in paragraph (1) do not apply, is classified of medium risk, and the Bank must take the required measures as stated in the provision relating to customer acceptance.
• Simplified measures are not to be taken in case of suspicious Money Laundering or Terrorism Financing operations or high risk circumstances.

**Third: Low risk customers**

• Each natural customer that does not have any commercial activities is of a low risk if none of the indicators mentioned in paragraphs (1) or (2) are present. For these customers, the Bank takes the mandatory measures regarding identifying the identity of the customer and the actual beneficiary as well as verification to the extent permitted as stated in the provision relating to customer acceptance.

• Simplified measures are not to be taken in case of suspicious Money Laundering or Terrorism Financing operations or high risk circumstances.

**Third: Customer diagnosis and analysis**

In diagnosing and analyzing customers' accounts, Bank of Jordan relies on the risk-based approach (RBA):

1. Generally, enhanced due diligence is performed and greater attention is given to high risk customers.

2. The need to obtain the approval of Bank of Jordan’s general manager or regional manager or whoever is authorized by the Senior Executive Management prior to establishing a relationship with customers of high risk (Politicians, Non-resident customers, charities, currency exchange companies, private banking customers, customer who belong or reside in countries which do not apply FATF recommendations or do not apply them sufficiently), in addition to any group that is categorized under customers of high risk pursuant to the instructions issued by the Compliance Department. This approval must also be obtained when discovering that a customer or an actual beneficiary falls under the category of high risk customers.

3. The necessity of taking adequate measures to ascertain the source of wealth of customers and actual beneficiaries who fall under any of these categories.

4. The necessity of constantly following up on these customers’ transactions with the Bank and exercising special care to business relationship and transactions conducted with them. This is in addition to ensuring that these transactions are consistent with the Bank's knowledge regarding the customer and the customer's activity pattern as well as the nature of risk, including if necessary the source of money and comparing it with the customer's peers in the same activity or with those who fall under the same category of risk level. All these data must be duly recorded and saved.

5. If the Bank notices that any of them are not clear economic transactions, necessary procedures to determine the surrounding circumstances of the business relationships and transactions that are carried out with any of these categories and their purpose must be taken. Records of these results are to be documented in the Bank's records.

6. Knowing the income sources of the account, the nature of the customer's activities and the expected account size in comparison with other accounts that have similar activity in the same area and with any other available factors.
7. The information obtained relating to customers, the nature of their activity, the type and size of the activity, as well as the place of work and the authorized agents, in addition to any other information the branch deems necessary are to be filed and recorded.

8. The customer profile should contain a specific part for all documents related to identifying the customer and any other documents supporting the transactions that are carried out within the scope of the Banking Relationship that are relevant to anti-money laundering and Terrorism Financing operations.

9. In the event the Bank is unable to perform customer due diligence, the Bank should not open an account or establish a Banking Relationship of any kind with the customer or perform any transactions on his account. Additionally, the Bank should immediately notify the Unit through the adopted channels in case there is suspicion of money laundering or Terrorism Financing.

10. No financial transactions are to be performed for any customer who does not have an account at the Bank, except for currency exchange transactions which are performed only through currency exchange offices that are subsidiaries of the Bank (occasional customers), with comparing the customer who is requesting the service's name with the names and entities listed on the embargo lists issued pursuant to the Security Council's resolutions.

11. In the event the currency exchange transaction or several connected transactions exceed the amount of JOD (10,000) ten thousands, the employee of the Bank at the currency exchange office shall fill and send a disclosure form in relation to occasional customers and to the Compliance Department / Anti-Money Laundering and Terrorism Financing Unit. The disclosure form shall include (the customer’s name, nationality, type and number of identity, permanent residency address, address in Jordan, phone number, transaction amount, source of money), in addition obtaining the necessary supporting documents to identify the legal person in the event the legal person is the beneficiary of the currency exchange transaction.

12. **Bank of Jordan permits postponing the verification procedures of the customer identity until after establishing the relationship in accordance with the following:**
   - The postponement of the verification procedures is essential to maintain normal business performance and such postponement does not cause risk of money laundering or Terrorism Financing.
   - The Bank performs the verification procedure within a maximum period of (10) days.
   - The Bank has implemented the necessary measures to manage the risks of money laundering or Terrorism Financing regarding the case postponed, which includes limiting the number, type and amounts of transactions that can be performed prior to conducting the verification procedures.

13. If, prior to conducting the verification procedures as stated in paragraph (12) above, the Bank establishes a continuous relationship with the customer, and the Bank is unable to perform the verification, the Bank shall terminate the relationship and immediately notify the division through the adopted channels in case there is a transaction that arises
suspicion of being linked with money laundry or Terrorism Financing, without permitting the customer to withdraw any cash after the relationship is terminated, and shall use other payment means that can be audit trailed.

14. The necessity of conducting all enhanced due diligence procedures in case a deposit in a dormant account is performed (by someone who is not the account holder or a representative by a power of attorney or a bank certified authorization), without changing the status of the dormant account.

**Fourth: Continuous monitoring of accounts and their operations** as per the risk based methodology.

4.1 Bank of Jordan performs continuous monitoring on all accounts regardless of the category of risk level.

4.2 The Bank adopted the risk-based methodology in determining the required level of care that should be exercised towards the customer.

4.3 By continuous monitoring and reviewing of accounts, a periodic risk score is conducted based on several factors, the most important of which are (categorizing the customer risk when opening accounts, the channels used by the customer to perform his financial transactions, the intensity and volume of the performed transactions in comparison with the nature of the activity, as well as the services provided to the customer and their rate of risk).

4.4 Based on the risk score of the customer, the level of care that should be exercised towards the customer is determined as well as identifying the necessary reinforcements which must be taken to justify the performed transactions.

4.5 Monitoring scenarios shall be programmed in the Anti-Money Laundry Profiling System based on the risk based methodology, and shall be continuously evaluated and amended based on the self-evaluating process of money laundry and Terrorism Financing in the entity as well as new money laundry and Terrorism Financing trends and methods.

4.6 **The following are cases that require special care in addition to the required due diligence as per the proportional importance of the risks**

4.6.1 If after establishing the Banking Relationship, the correctness or accuracy of the customer's identification data are doubted and any discrepancy results from comparing the transactions performed on the account with the disclosure of the customer at the time the account was opened in relation to the money's source, the size of the deposits and income...).

4.6.2 Unusual complex and large transactions in comparison with the customer's usual account transactions.

4.6.3 Any other unusual transaction that has no clear economic justification or that is incompatible with the nature of the client's risk and activity.

4.6.4 When there is an obvious change in the account management method.

4.6.5 When the Bank realizes the lack of information regarding one of the customers.

4.6.6 When a correspondent account is opened.
4.6.7 When facilities against deposits are requested.
4.6.8 When leasing safe deposit boxes.
4.6.9 When cash or cheques are deposited into an existing account through a person(s) who do not represent the account holder with a power of attorney, or an authorization certified by a bank.

4.7 Taking all necessary measures to determine the background of the circumstances surrounding any of the business relationships with the high risk customers and check their source of wealth.
4.8 Paying attention to the transactions and operations that are not compatible with nature of the account, the size of the declared income or the nature of the activity as per the abovementioned patterns and indicators of Suspicious Transactions (the extent of compatibility of the transactions with the customer’s professional activity or habits or personality).
4.9 Linking the nationality of the customer, purpose of residence, internal and foreign sources of income and the customers expertise in his field of profession.
4.10 Linking between the type and nature of the relationship of the account holder and his agent or the authorized account operator.

7. Know Your Employee Policy

Implementing the know your employee principal (KYE) is one of the most important matters that need to be considered when hiring any of the bank’s employees, given the significant human role represented by the employees in combating or facilitating Money Laundering and Terrorism Financing operations. As banking business is based on specific traditions and ethics which are at the same time an integral part of the public traditions and ethics, the Bank recognizes the risks of employees having access to information and the importance and sensitivity of these information, in addition to the authorities and powers granted to them.

Accordingly, a bank employee, as a member of the community, should be a bright and trustworthy example of high morals. Moreover, his public and private relationships should serve as a confirmation of these qualities, he should also distance himself from any citizen who raises suspicion, financial confusion or job exploitation. The employee should also make every possible effort to provide premium banking services.

The fine selection of employees whilst taking into account their curriculum vitae, especially those with direct interaction with clients and focusing on their personal traits such as intelligence, quick-wittedness, alertness and caution...etc. and closely monitoring new banking employees is an important factor to consider due to its effectiveness in discovering Suspicious Transactions conducted by them in early stages. As such, the policies and procedures, job description, internal monitoring procedures, recognition of powers, compliance with laws and instructions, the Code of Professional Conduct, bilateral oversight and other deterrent matters should be the basis for employees when performing their jobs.
Bank of Jordan applies the know your employee policy through two primary focus points as follows:

The first focus point is prior to recruitment:

In this focus point, the human resources department receives job applications for new candidates as per the standard form prepared for this purpose (KYE form), and the following matters are verified:

- The candidate is not listed on any of the global ban lists.
- The candidate has not been listed on any of the blacklists in the Unit of bounced cheques.
- The candidate is not listed in any of the prohibited customers.
- CRIF Credit inquiry results.
- Determine whether the candidate has any relatives working in the Bank and specifying the degree of relativity.
- Determine if there are any other sources of income for the candidate.

The second focus point is verification of existing employees:

In this focus point, the know your employee policy (current employees) is implemented and the following procedures are taken:

- Reverifying the procedures that were taken in the first focus point.
- Continuous monitoring and reviewing of the financial transactions performed on the employees' accounts within certain scenarios specified in the AML Profiling System.
- Monthly scanning of the employees' accounts on the global ban lists and verifying that none of the current employees are included in these lists.
- The results are presented to the personnel cases verification committee for the purposes of examining the results and sending the recommendations to the compliance committee/ Board of Directors.

Behaviors that may indicate employee's involvement in money laundry and Terrorism Financing:

Some behaviors are considered as an indicator of the bank employee's direct or indirect involvement in money laundry and Terrorism Financing as the employee can offer his assistance through receiving deposits and transferring them to another party or through intentional negligence in checking the customers’ good-faith or the correctness of their information when opening accounts. Hereunder some of these behaviors are listed:

1. The spending level of the employee rises significantly in a manner incompatible with his monthly income.
2. The employee avoids taking any leaves or holidays.
3. The employee constantly bypasses monitoring procedures and follows an elusive policy while performing his work.
4. The employee assists in performing transactions with unknown final beneficiary or the counterparty is completely anonymous.
5. Employee exaggerates in the transparency, morals and financial sources of the customer in his reports submitted to the bank’s management.

8. **Principals to be considered when executing credit and debit transactions.**

**First: cash deposits:**
1. In the event a customer wishes to make a cash deposit within the ceiling set by the Bank, the teller employee at Bank of Jordan is obliged to fill in the specified fields on the source of money screen which appears on the banking system, including (the purpose of the deposit, sources of the deposited cash, the relationship of the depositor with the account holder, type and number of the document, date of birth, the party to which the depositor belongs to).
2. Request from the customer to submit supporting documents proving the sources of the deposited money pursuant to the instructions of the compliance department and obtain a copy of these documents and file them.
3. In case the documents proving the sources of the money are not available with the customer, the deposit transaction must be accepted while confirming to the customer the necessity of providing the Bank with the requested documents, and notifying the compliance department in writing if the customer is unresponsive after exercising reasonable efforts in following up with him (provided that the period does not exceed (10) business days).
4. In case the customer hesitates or withdraws from performing the cash deposit transaction after the employee requests information regarding the source of the cash, the branch employee must fill a suspicion form and send it to the Anti-Money Laundering and Terrorism Financing division. Also, employees must obtain the personal ID’s of customer making cash deposits when carried out by persons who do not carry an authorization permitting them to deposit in the account.

**Second: Transfers:**
1. **Outgoing transfers:**
a. Refrain from providing transfer services to non-customers of the Bank, with the exception of cheques ordered for governmental entities or bodies.
b. Bank of Jordan conducts enhanced due diligence in regards to the customer requesting the issuance of the transfer with verifying that all information required are provided within locked fields that are not amendable prior to issuing the transfer. These fields include name of issuer, IBAN number, name and address of the transfer beneficiary bank, the amount in the original currency, the equivalent in JOD, date, purpose, the relationship between the transferor and the beneficiary, the national number for Jordanians, and the nationality of non-Jordanians as well identification documents. All these information are to be filed in the banking system.
c. Obtain approval of the compliance department prior to issuing a transfer to countries of high risk which are specified under the instructions issued by the compliance department.
d. Refrain from issuing single pack transfers and rather issuing individual transfers for the customers of the Bank.
e. Auditing all outgoing transfers regardless of the amounts within the banned lists (EU, UN, OFAC, etc.)
f. Transfers issued upon the request of customers holding bank accounts must be performed through the customer’s account. In case of payments are to be made in cash, these payments must be performed through the customer’s account.

2. **Incoming transfers**
   a. The Bank shall not receive any transfers that are not for the customers of the Bank.
   b. Auditing all incoming transfers regardless of the amounts within the banned lists (EU, UN, OFAC, etc.)
   c. Bank of Jordan provides efficient and effective auditing systems for verifying information regarding incoming transfers fulfilling the required information including the name and address of the issuance requester, IBAN number, receiver of the transfer, and the purpose of the transfer.
   d. The Bank adopted the risk-based methodology regarding transfers that have missing information relating to the issuer or the beneficiary, by requesting the missing information. In the event the missing information is not provided; measures shall be taken based on the assessment of the degree of risk including performing, suspending, or refusing the transfer, provided that this is a reliable indicator in the Bank’s assessment of the extent of suspicion in the transaction.
   e. The Bank shall take adequate verification procedures of the beneficiary's ID and shall file this information for a period of not less than five years.
   f. All incoming transfers for customers of the Bank that are of a different currency than the currency of the account are to deposited in the customer account after being exchanged to the account’s currency. These transfers should not be paid in cash.

3. **Responsibilities of the intermediary bank:**
   In the event the Bank participates in performing the transfer without being the issuer or receiver, the following must be focused on:
   A. The information that are attached to the transfer shall remain when executing the transfer.
   B. In the event the Bank is unable to maintain the information attached with the transfer for technical reasons, the Bank must file the information as received for a period of five years regardless of the completion of these information. This is being for the purpose of responding to receiving bank's query regarding the transfer within three days of the date of query.
   C. In case the information was inadequate in relation to the issuer of the transfer, the intermediary bank is obliged to notify the Bank receiving the transfer when performing the transfer and to file the available information for a minimum period of five years.

4. **Outgoing and incoming electronic transfers exceeding seven hundred Jordanian Dinars or its equivalent in foreign currencies shall be subject to the same instructions for manually performed transfers.**
Third: Cheques

1. In the event a customer requests to deposit a cheque in an account, the employee must fill in the fields related to the issuing bank, the name of the withdrawer, the amount, the date and purpose. These fields are to be filled in the deposit voucher before printing.

2. In the event the customer requests cash withdrawal/ cheque withdrawal for the benefit of himself, the employee must fill in the fields related to the date, the amount and purpose of the transaction.

3. In the event the customer requests to execute a transaction for the withdrawal of a cheque from the account/ cash, the employee must fill in the fields related to the date, the amount/ the bank of the beneficiary, name of the beneficiary, the relationship with the account holder, and the purpose of the transaction.

4. Stating the bank of the beneficiary, name of the beneficiary, amount, date, the purpose of the withdrawn checks from the account/ offsetting.

5. Input all information on the banking system.

Fourth: Internal transfers:

Performing due diligence procedures in relation to the customer requesting the internal transfer between accounts to verify the adequacy of the requested information related to him prior to the transfer, including the name of transferor, the name of the beneficiary, the relationship between the transferor and the account holder, the amount, the transfer date and purpose, and input all information into the bank system.

9. Requirements for dealing with foreign banks.

- Fulfilling the customer identification requirements (foreign bank) and obtain the required documents showing the legal status of the bank requesting the opening of the account, the public and private ownership of the bank, names of shareholders who hold more than 5% of the capital of bank.

- The nature of the foreign bank's activity and its reputation in the field of anti-money laundry and Terrorism Financing, work locations and the purpose of opening the account.

- Information regarding the bank’s management (the names of the executive management, their qualifications and expertise...etc.).

- Obtain the general manager’s approval for establishing a relationship with a foreign bank.

- The status of monitory and supervision on the bank in the country in which it operates, and to refuse to open an account for a bank registered in a country without having physical presence therein, or which is not subject to the supervision of the Shell Bank authorities.

- The Bank takes sufficient procedures to assess the anti-money laundry and Terrorism Financing policies, procedures, systems and regulations applied by the foreign bank, so as to be able to formulate a belief that the foreign bank prohibits using his accounts by a Shell Bank or performs transactions linked with Money Laundering or Terrorism Financing. This is necessary as well to establish a relationship with the foreign based on a clear understanding of each party's responsibilities towards Anti-Money Laundering and Terrorism Financing. In the event it appears that the foreign bank has transactions with Shell Banks, the Bank is obliged to not enter or continue with the Banking Relationship.
- Ensure that the foreign bank has performed the mandatory due diligence procedures regarding its customers (KYC) who are authorized to use Nested Accounts/ Downstream/ Upstream/ Clearing/ Payable Account*.
- Ensuring the foreign bank is able to provide information related to those customers and the transactions performed on these accounts when required.
- To confirm in writing to Compliance Department that these requirements are implemented when opening accounts for foreign banks, prior to performing the transactions.
- Continuously updating and reviewing this information in coordination with the Compliance Department and Financial Institutions division.

10. Mechanism of Identifying and Reporting Suspicious Transactions

1.1 How to identify Suspicious Transactions
- With the correct understanding of the pattern of Suspicious Transactions and with good knowledge of the nature of the customer’s activity and the volume of his income, when dealing with a customer or performing a transaction or examining notable bank statements and comparing them with the customer’s transactions, an employee might sense that there is something unusual or unjustified.
- If the employee has suspicions based on unacceptable grounds, he is entitled to discuss the situation with the manager or the assistant manager, as the customer might perform unusual transactions that are legitimate and do not involve illegal activity.
- Knowing the customer well and having information and data relating to the nature of his business, the volume of the activity, income sources, dealing history and other information is the only way to dispel or strengthen doubts.

• The questions that must be always ready:
  1. Does the transaction conform with the customer’s professional or personal activity?
  2. Is the transaction volume at the same level that the customer regularly deals with?
  3. Are there recent changes in the nature, quality or volume of the transactions?
  4. Are there any justifications for the foreign transaction as to being linked with relationships of the customer’s business or himself, and is the country categorized under uncooperative countries or countries where Money Laundering or drugs are widely spread ...etc.?

1.2 Mechanism of reporting Suspicious Transactions

If the answers to the above questions leads to the employee's belief that there is suspicion of Money Laundering or Terrorism Financing, the following must be done:

1. Fill a suspicion form regarding the Suspicious Transaction related to Money Laundering proceeds or used for Terrorism Financing purposes.

* In the event Bank of Jordan opens an account for a foreign bank, and the foreign bank has permitted for some customers to act through this account by any method of payment, Bank of Jordan is to ensure that the foreign bank has performed all necessary (KYC) procedures regarding the said customers.
2. Prepare sufficient data and information relating the customer and the suspicious case by referring to the customer’s file and query methods available at the branch, all are to be attached with the transaction.

3. Forward the case with its attachments to the liaison officer for his examination and approval.

4. The liaison officer is responsible of reviewing the suspicious case along with its attachments and to then submit it to the anti-money laundry and Terrorism Financing Unit for them to make a decision.

5. In the event there are any obstacles that may prevent the employee from reporting the suspicious cases such as fear of the direct manager or any other reason, it is possible to report through early reporting mechanism on the designated email.

6. The employee of the anti-money laundry and Terrorism Financing Unit will receive the suspicious case with its attachments for examination and analysis, and he can request additional information if required, and then submits the case to the Money Laundering Reporting Officer (MLRO).

7. The Money Laundering Reporting Officer (MLRO) reviews and examines the entire case.

8. If the Money Laundering Reporting Officer (MLRO) is convinced that there is in fact suspicion, he submits the suspicion reports (SAR/STR/UTR) with supporting files and documents to the competent authority (the anti-money laundry and Terrorism Financing Unit) through the designated channels.

9. If the Money Laundering Reporting Officer (MLRO) is unconvinced of the sufficiency of the reasons raising suspicion, the documents shall be filed whilst the case remaining under surveillance for six months, based on the surveillance results; a suspicion report (SRA/STR/UTR) will be submitted due to the presence of strong suspicion justifications, or the customer is removed from the list of customers under surveillance.

10. All files and documents related to cases that were subject of SAR shall be filed for a period of five years from the notification date or until a court ruling is issued, whichever is longer.

11. Every employee in the Bank shall maintain the confidentiality of the information stated in the notification information and shall not disclose any of it to any one including the suspected customer, and shall ensure that no actions that might alert or tip off the suspected customer of the notice sent to the Unit are taken, otherwise the employee shall be subject to legal consequences.

12. The compliance department shall constantly remind the employees fulfilling all job positions of the Bank about their responsibilities in reporting any suspicious cases or unusual behaviors and designate channels that assist the employees in these matters through (Whistle Blow) and direct contact with the Money Laundering Reporting Officer (MLRO).

11. Reporting channels

Bank of Jordan shall provide numerous reporting channels for any suspicious indicators regarding money laundry and Terrorism Financing transactions that might appear to any employees of the Bank regardless of the employee’s job description, through the following:

- The direct manager.
- The direct manager, who in his turn notifies the compliance department.
If you feel that the authorities, you choose to notify have not addressed the situation and the practice remains, you must resort to the whistle below system (Whistleblow@bankofjordan.com.jo) or by directly sending a letter to the compliance department while taking the following into account:

1. List the reasons that led to the suspicion of the case.
2. Detailed explanation of the case.
3. Mention the parties related to the violation.
4. Provide the compliance department of any evidences, suggestions, recommendations that would assist in evaluating the case.

12. The duties and responsibilities of the Board of Directors.

1. The Board of Directors is to approve the policy of Anti-Money Laundering and Terrorism Financing transactions, upon the recommendation of the competent committee (the compliance committee).
2. Review the reports submitted by the compliance department / anti-money laundry and Terrorism Financing Unit concerning actions taken to combat money laundry and Terrorism Financing.
3. Review the periodic reports relating to unusual and Suspicious Transactions or transactions that are suspected of being linked with Money Laundering and Terrorism Financing.
4. Appoint a Money Laundering Reporting Officer (MLRO) and his deputy, and obtain a no-objection letter from the Central Bank on their appointment after the compliance committee/Board of Directors have confirmed that they possess the required qualifications. The details of Money Laundering Reporting Officer (MLRO) and his deputy must be provided to the anti-money laundry and Terrorism Financing Unit (FIU Unit) following obtaining approval of the Central Bank of Jordan.
5. Determining the powers and authorities of the Money Laundering Reporting Officer (MLRO), provided that they include as a minimum enabling him to practice his duties and responsibilities independently and in a manner that ensure maintaining the confidentiality of the information and procedures he takes, and for that to be fulfilled, he is to have access to the records and data needed for him to perform his job.
6. Obtain the approval of the Central Bank of Jordan for the resignation or ending the services of the Money Laundering Reporting Officer (MLRO) or his deputy.
7. Adopt policies, procedures, and disciplines to ensure the existence of highest standards when appointing employees, for the purposes of verifying the suitability of the executive management, the Money Laundering Reporting Officers (MLRO), and those other employees involved in combating money laundry or Terrorism Financing.
9. Adopt the appropriate mechanisms thereby enabling both the internal auditing staff and the compliance director to verify compliance with the instructions, policies and procedures that are in effect to combat Money Laundering and Terrorism Financing transactions, subject to coordination with respect of determining the powers and responsibilities.
13. Duties and Responsibilities of the Senior Executive Management

- Prepare the Anti-Money Laundering and Terrorism Financing policy for the Bank of Jordan Group, as well as the results after having it reviewed, and any suggested amendments. In addition to submitting the recommendations to the compliance committee/Board of Directors to approve the amendments in preparation of obtaining approval of the Board of Directors.

- Prepare reports regarding internal monitoring and controlling procedures in relation to Anti-Money Laundering and Terrorism Financing, in addition to any challenges that may prevent the said monitoring or controlling and submit the reports and recommendations to the Board of Directors.

- Adopt detailed written procedures to combat Money Laundering and Terrorism Financing, which written procedures must accurately determine the duties and responsibilities in accordance with the approved policies. Instructions issued by the Central Bank of Jordan in relation to this matter are to be considered.

- Allocate an independent annual budget (to be approved by the Board of Directors) to finance trainings and attend workshops related to anti-money laundry and Terrorism Financing for the employees of the Bank, and to provide systems that assist the compliance department in performing its duties.

- Perform self-evaluating assessments for the risks of Money Laundering and Terrorism Financing at the level of the Group pursuant to the methodology approved by the Bank for this purpose, the results of which shall be submitted to the compliance committee/Board of Directors.

- Reviewing the risk of Money Laundering and Terrorism Financing / its origin file whilst cooperating with the market operations and risk department, and amending them to reflect any developments that may arise and affect the risks faced by the Group, (issuing new products, creating channels of service delivery, attracting new customer segments, opening branches in high risk areas) and approve the amendments results by the competent board committees.

14. Duties and responsibilities of the Anti-Money Laundering and Terrorism Financing Unit.

1. Reviewing the Anti-Money Laundering and Terrorism Financing policy for the Bank of Jordan Group, and submitting the recommendations to the compliance department.

2. Providing the director of the compliance department with the necessary monitory checks to examine the Money Laundering and terrorist financing risk file/origin for the purpose of conducting a self-assessment of Money Laundering and Terrorism Financing risk/origin.

3. Accessing the AML Profiling System to review the compliance officer’s comments and evaluate if these comments justify the performed financial transaction and take appropriate measures in relation thereto.

4. Request the liaison officers to provide the Unit with detailed reports regarding customer’s activities, and the files and documents that prove the nature of the activities.

5. Prepare detailed reports on Suspicious Transactions and submit them to the Money Laundering Reporting Officer (MLRO) for examination and resolving thereupon.
6. Respond to any inquiries received from the Anti-Money Laundering and Terrorism Financing Unit or from the Central Bank of Jordan and provide them with the required details and information.

7. Receive the branch's inquiries regarding business services transactions and outgoing/incoming transfers from and to countries of high risk, in addition to collecting cheques exceeding the amount of JOD 100,000 or its equivalent in foreign currencies and attach them on the inquiry form, respond to them and submit them to the Money Laundering Reporting Officer (MLRO) for approval.

8. Prepare recommendation reports on the results of the analysis and of all data and documents required in the Know Your Customer (KYC) for customer who belong to countries of high risk or fall under the categories of politically exposed politicians, Non-resident institutions and any other categories imposed by the instructions, and submitting the recommendations to the director of the Unit in order to obtain the final approval.

9. Conduct training courses for the employees to raise awareness concerning Money Laundering and Terrorism Financing transactions and methods of combating them in accordance with the training schedule approved by the training Unit and awareness campaigns.

10. Monitor the automated system and constantly update the list.

11. Follow up with Financial Institutions division when responding to queries of correspondence banks.

12. Responding to questionnaires received from foreign banks to assess the Bank’s compliance with the Anti-Money Laundering and Terrorism Financing laws and instructions.

13. Following up with global developments in money laundry and Terrorism Financing trends, combating procedures especially those issued by the international committees FATF, International Monetary Fund, International Bank for Reconstruction and Development, the Basel Committee and any Anti-Money Laundering and Terrorism Financing national committee and other international organizations, and suggesting recommendations to ensure compliance with any instructions issued by these committees.

14. Review the international sanctions program’s data base prepared by the Unit and constantly updating it, in addition to reflecting the procedures that are to be followed to avoid any breaches.

15. Verify the compliance of corresponding banks with the Anti-Money Laundering and Terrorism Financing laws and instructions.

15. Duties and Responsibilities of the Liaison Officer.

In the aim of organizing the working mechanism and determining the responsibilities in combating money laundry and Terrorism Financing, a compliance officer has been appointed in all Bank’s divisions (branches, business development centers, relationship management officers in the business development unit, follow up unit, collection unit, human resources unit, (compliance coordinator), and the compliance department is entitled to appoint a compliance officer in any unit of the Bank for the purposes of meeting its requirements.

It is not the compliance officers' responsibility to investigate and check if the money is illegal, rather their responsibilities are limited to exercise reasonable effort and prepare reports on suspicious cases
depending on the available data and information obtained regarding the customer’s activity. Therefore, the compliance officer is appointed to perform the following:

**Duties of the compliance officer in branches, business development centers and human resources**

1. Accessing the automated system for Anti-Money Laundering and Terrorism Financing on a daily basis and examining the customer alerts in terms of the purpose, source of money and the compliance degree of the transaction with the nature and volume of the customer’s activity by reviewing the history of the customer’s transactions.

2. Confirm the results of the investigation on the alerts to the automated system pursuant to point (1) and automatically send them to the compliance department / Anti-Money Laundering and Terrorism Financing Unit.

3. Provide the Anti-Money Laundering and Terrorism Financing Unit / the compliance department with the necessary reports, documents and files relating to the customers in question.

4. Prepare a detailed report about the suspicious customers and accounts while stating the justifications for the suspicion and attaching all supporting documents.

5. Receiving suspicious cases sent by the employees in relation to customers’ behaviors as well as the justifications of suspicion, and preparing a suspicion case and submitting it to the compliance department / Anti-Money Laundering and Terrorism Financing Unit.

6. Meet the requests of the Anti-Money Laundering and Terrorism Financing Unit and respond to their inquiries.

7. Support and help the compliance department through training the compliance officers and front desk employees.

8. Conduct supervisory checks for controlling Money Laundering and Terrorism Financing risks associated with the work of each unit/department/branch the risk profile of each.

**16. Duties and Responsibilities of the Money Laundering Reporting Officer (MLRO).**

1. Receive information and reports regarding unusual and Suspicious Transactions or cases that are suspected to be linked with Money Laundering and Terrorism Financing, examine them and take the appropriate decision regarding submitting the suspicion report to the concerned authority (Anti- Money Laundering and Terrorism Financing Unit), or closing these cases provided that the decision to close is justified.

2. Maintain all documents and reports received for a minimum period of 5 years, whether the decision of submitting the suspicious report has been taken or it has been closed without notification.

3. Provide the Unit and the competent authorities with the relevant data relating to Suspicious Transactions that are linked with Money Laundering or Terrorism Financing, and any other requested information, and provide easy access to the relevant information and records for the purpose of performing their tasks.

4. Prepare periodic reports for submission to the Board of Directors in relation to suspicious and unusual transactions or that are suspected to be linked with Money Laundering and Terrorism Financing.
5. Provide the Central Bank of Jordan with the updated obstacles that prevent implementing the procedures in foreign branches whether the requirements of a foreign country are lesser or stricter than the requirements of Jordan.

6. Ensure that the employees are fully aware of the practical procedures and policies of anti-Money Laundering and Terrorism Financing transactions.

7. Provide means to ensure the updating of the list of international sanctions programs, the list of non-cooperating countries and the ban list of the Security Council's resolutions.

8. Continuous updating of the latest developments related to Money Laundering and Terrorism Financing transactions and ways to monitor and combat them.

9. Discuss the employees training plans in relation to Anti-Money Laundering and Terrorism Financing.

10. Provide the Central Bank of Jordan at the end of each year with a survey illustrating the training courses and workshops that the employees have attended during the year, and their costs.

11. Immediately inform the Unit if a suspected customer requests to close his account/ accounts, without permitting the customer to withdraw the amount in cash and rather permitting him to use any other Audit-trail payment methods.

12. Investigating the Suspicious Transactions and notifying the competent authorities if necessary.

13. Prepare customized profiles for Suspicious Transactions related to Terrorism Financing or to any persons included on the lists, in which photos of the notifications of these transactions and relevant data shall be filed.

14. Suspicious reports that are submitted by the Anti-Money Laundering and Terrorism Financing Unit are not deemed as a breach of the banking secrecy.

15. Prepare reports regarding the internal Control and monitory procedures in the field of Anti-Money Laundering and Terrorism Financing and any obstacles that might prevent submitting the reports and the recommendations to the Board of Directors.

17. **Duties and Responsibilities of the Internal Audit Department.**

The Internal Audit Charter includes within its main functions the following:

1. Continuous verification, review and update the policy of Anti-Money Laundering and Terrorism Financing by the compliance department, as well as verifying the Control and monitory systems in the compliance department that are related to risks of Money Laundering and Terrorism Financing transactions.

2. Designate independent and qualified staff within the internal auditing department, supported with adequate resources to examine the compliance with policies and internal Controls, and anti-money laundry and Terrorism Financing procedures.

3. Designate an appropriate verification mechanism to ensure compliance with the set procedures, policies and instructions by the competent auditing staff and the compliance manager, to combat Money Laundering and terrorism finance, subject to coordination in determining authorities and responsibilities between.
4. Evaluate the results of self-assessment process of the risks of Money Laundering and Terrorism Financing / its origin which were performed by the director of the compliance department and submit the recommendations to the competent board committees.

5. Participate in preparing/ reviewing the risk profile of Money Laundering and Terrorism Financing / its origin and cooperating with the compliance department and the market risk and operations unit, as well as verifying that there are mitigating procedures for all Money Laundering and Terrorism Financing risks that the Group encounters.

6. Verify the results of the self-assessment process that are performed by the manager of the branch/ unit on the risk profile of the branch/ unit that is under his supervision, and reflect the assessment on the internal auditing reports that are submitted to the auditing committee/ Board of Directors.

18. Reviewing and approving the Anti-Money Laundering and Terrorism Financing policy.

- The compliance management/ general management (parent institution) is responsible for reviewing this policy annually and amending it if required.
- The Board of Directors, represented by the competent committees, is responsible for approving the policy and any amendments made to it.
- This policy is considered the Master Policy for Anti-Money Laundering and Terrorism Financing matters in relation to all members of the Bank of Jordan Group, including foreign branches and subsidiaries, and represent the main guidelines that are to be complied with. A due consideration is to be given to the hosting country's laws and instructions in which the foreign branches or subsidiaries are located. If any of the terms of these policies contradict with the hosting country's laws and instructions in which the foreign branch or subsidiaries are located, the stricter instructions are to be implemented.
- Pursuant to this policy, in the event that the laws governing issues related to Anti-Money Laundering and Terrorism Financing contradict with this policy, the foreign branches and subsidiaries are permitted to create a policy emerging from this policy in a manner compatible to the hosting country's laws, which shall hereby be deemed to have been approved by the Board of Directors without the need to obtain the approval of the general management (parent institution), in accordance with the following:
  1. The compliance department / Anti-Money Laundering and Terrorism Financing Unit in the Group/ foreign branch operates pursuant to the compliance requirements of the Anti-Money Laundering and Terrorism Financing instructions by setting and approving the sub-policy in accordance with the corporate governance principles applying to such institution/ foreign branch.
  2. Continuously coordinating with the compliance department of the parent institution through constantly notifying them about any developments and aligning the policies and sub-policies.
  3. The compliance officer shall ensure that such amendments do not contradict in any way with the instructions issued by the Central Bank of Jordan, and that they do not hinder the implementation of any requirements of the Central Bank of Jordan.
4. Sub-policies which meet and align with the requirements of the laws of the hosting countries and that are emerged from the master policy, are deemed automatically approved by the Board of Directors. Such approval shall be deemed given as part of the previous resolutions issued by the Board of Directors to approve the master policy.

19. Training and Qualifying Employees

Training is one of the important factors in the formula of Anti-Money Laundering and Terrorism Financing, it is the tool that enables the employees to understand the nature, type and ways of Money Laundering and Terrorism Financing. Training also provides appropriate necessary information in regards to the local and global developments on Money Laundering methods and how to combat it. Additionally, it prevents employees from being victimized by persons carrying out Money Laundering and Terrorism Financing transactions. The clear understanding of Money Laundering and Terrorism Financing methods and ways to detect them allows employees to positively cooperate and motivate themselves to exercise their responsibilities of protecting the Bank’s reputation and avoid using the Bank as a channel by money launderers. Therefore, the following must be taken into account:

- Prepare and implement a continuous training program for all employee regardless of their job position or administrative positions in relation to Money Laundering and Terrorism Financing and methods to combat it.
- Familiarizing employees with the method of notifying unusual transactions.
- Conduct training workshops that are commensurate with the employees’ levels according to the nature of their job.
- Follow up on training programs and local and foreign publications in relation to this matter to pursue the latest developments and amend the training modules to align with them.
- File all records of the training programs that were conducted within the period of 5 years as a minimum, including names of the trainees, their job descriptions, their qualifications and the entity that performed the training whether inside or outside the Kingdom.
- Subject all new employees to training programs in the field of Anti-Money Laundering and Terrorism Financing during the first year of their employment.

20. Updating data.

Bank of Jordan implements procedures to regularly update the data of its customers (account holders and authorized representatives) at least every two years pursuant to the risk-based approach in order to ensure that the Bank’s records are regularly updated and renewed. This is in addition to the importance of promptly implement the update in the following cases:

- When performing transactions in large amounts or using banks tools in an unusual way.
- When a fundamental change occurs to the customer’s information documentation mechanism.
- When a significant change occurs in the method of managing the account.
- When the Bank realizes that it does not have adequate information regarding one of those customers.
- When there are reasons for an update, or there are doubts in regards to the correctness or adequacy of the previously obtained information, or when a fundamental change occurs to the account management method.

In the event that the customer does not update his information pursuant to the Bank’s policy, some of the financial transactions and services provided to the customer are to be gradually stopped until the customer updates his information. Noting that the Bank has implemented adequate procedures to urge customers to effect the update by activating tools and awareness campaigns for customers on the consequences of not updating their data.

21. **Documents and record keeping.**

1. Records and documents supporting ongoing relationships and banking operations must be kept for a period of 5 years at least from date the transaction was performed, or the relationship was terminated, as the case may be.
2. The customer’s file must include all documents and data concerning the identification of the customer and any documents relevant to the monitoring or combating of anti-terrorism and Money Laundering.
3. Prepare a file specifically for transactions that are suspicious to be connected with Money Laundering or Terrorism Financing, where copies of the notifications of transactions, documents and data related to them shall be saved. These profiles shall be saved for a period not less than (5) years from the date of notification or until a court ruling is issued, whichever is longer, and is kept in the custody of the Money Laundering Reporting Officer (MLRO).

22. **Security Council resolutions.**

Bank of Jordan is committed to implementing the responsibilities stated in the mandatory relevant international resolutions, including all relevant resolutions under chapter seven of the United Nations charter.

Moreover, the Bank abides by the lists issued by the Technical Committee deriving from the national committee which applies the Security Council's resolutions regarding Anti-Money Laundering and Terrorism Financing relating to terrorist and Terrorist Organizations. **For this purpose, the Bank performs the following:**

22.1 Referring to the lists of the Technical Committee in order to verify the names contained in the list (and which are prohibited to deal with) pursuant to the Security Council Committee resolutions, whether by way of adding, modifying or deleting when performing any transaction or prior to entering into any new relationship with any person to ensure that the person’s name is not included on the list.

22.2 In the event the name of a person or an entity appears to match or is similar to a name that is included in the List made by the Technical Committee, the Bank applies the following procedures:
- Freeze the money and personal economic sources immediately with no delay, and shall immediately notify the Technical Committee of the procedure taken in this regard.
- Inform the Technical Committee of the existence of a bank account for the Terrorist Organizations, for the technical committee to take appropriate action.
- Immediately provide the Technical Committee with any information that may be of help in complying with the provisions of these instructions and in particular information relating to the money and economic sources owned, belonging to, or controlled by the Terrorist Person or Terrorist Organizations or any person that works for them or on their behalf.
- Any amounts, resulting from contracts or responsibilities that were entered into before the person was added to the ban list, will be credited to the dormant accounts, including profits and interests, provided that all of these amounts are subject to freeze.
- The Bank allows to credit any amounts or transfers in any accounts that have been subject to the freeze, provided that these added amounts be made subject to the freeze and the Technical Committee is immediately informed of these operations.
- The Bank is prohibited from making available any money or Economic Resources whether directly, indirectly, fully or jointly, to a terrorist or a Terrorist Organization listed by the Technical Committee, or for the benefit of either of them, subject to legal liability.
- In the event the Technical Committee approves the removal of a name from the list, the freeze on the money and the Economic Resources shall be lifted and the relevant person or his representative shall immediately be allowed to use the money and the Economic Resources, provided that the Technical Committee is informed of the action taken in this regard.


Bank of Jordan adopted the Control Risk Self-Assessment methodology (CRSA) for the purposes of identifying and measuring the risks of Money Laundering and Terrorism Financing that may be encountered within three basic levels (defense lines) as per the following:

1. **Defining Money Laundering and terrorist financing risks.**

   By identifying and understanding these risks at each level of the customer’s risk levels (existing and new), risks of countries and geographic regions, risks of products, services and operations, risk of service delivery channels, risks of employee, risks of correspondence bank noting that (68) group level risks were identified.

2. **Evaluating risks of Money Laundering and Terrorism Financing.**

   Risks of Money Laundering and Terrorism Financing were evaluated based on the principles adopted by the Bank to evaluate operation risks as follows:

   2.1 **Assets affected by the risks:** the Bank has identified the assets that are affected by the risks of Money Laundering and Terrorism Financing, and has arranged them according to importance and priority of mitigating risks affecting the assets, as follows:
   
   - Reputational risks.
   - Compliance/ reputation.
   - Financial assets/ legal risks.
➢ Compliance/ cash risks.
➢ Cash/ profit/ financial assets risk.
➢ Compliance risks (legal status of the bank/ legislation) risks.
➢ Information risks.
➢ Knowledge risks.
➢ Fixed assets risks.

2.2 Value impact of the asset: so that the value of impact on the Bank if exposed to Money Laundering and Terrorism Financing is determined, noting that Bank of Jordan has set zero tolerance degree for Money Laundering and terrorist financing risks within the documentation of risk appetite.

2.3 Likelihood of risk occurrence: the likelihood of risk occurrence was classified into (low, medium, high) and such classification is made on a case by case basis as per the relevant risk data.


Controlling the risks of money laundry and Terrorism Financing through surveillance systems that work to prevent or avoid the risk and/or the possibility of occurrence. The compliance department aims by coordinating with the market risk and operations unit and the auditing department to ensure that there are no risks uncontrolled by the surveillance procedures. Moreover, it is the compliance department’s responsibility to continuously develop and enhance these procedures.

This methodology is implemented through three main levels

➢ The first level: whereas the risks of Money Laundering and Terrorism Financing and the implemented surveillance procedures have been identified for the purpose of reducing the risks at the level of each division/ unit of the Bank’s units within the risk profile of each division/ unit as the first line of defense.

➢ Second level: prepare an AML Risk Profile for the risks of Money Laundering and Terrorism Financing at the level of the Bank as the second line of defense, that includes the following:
  • Risks of new customers.
  • Risks of current customers.
  • Risks of products.
  • Risks of dealing with foreign banks.
  • Risks of service providing channels.
  • Risks of employees.
  • Risks of countries and geographic areas.
  • Risks of subsidiary branches.

➢ Third level: preparing Corporate Risk Profile in which the risks of Money Laundering and Terrorism Financing are defined and listed among the main risks that the Bank could be exposed to on a strategical level, as the third line of defense.
Operations risk profiles must be evaluated at all levels when there is any change to the risks that the Bank is exposed to at least directly or annually, and duly approved and ratified by the Board of Directors. Moreover, self-assessment on all levels is to be conducted for the risks of Money Laundering and Terrorism Financing and the efficiency of the implemented procedures to Control the risks of Money Laundering and Terrorism Financing.

**Periodic evaluation of the Bank’s monitory environment:**

Perform a self-assessment of the risks of Money Laundering and Terrorism Financing operations and the efficiency of the procedures implemented to mitigate this risk on all of the previously mentioned levels with accordance to the following:

The first level (the risk profile at the level of each unit at the Bank):

This profile is being examined and assessed through performing a self-assessment that is carried out by the director of each department or unit.

The second level (the risk profile for Money Laundering and Terrorism Financing at the level of the group):

This profile is being assessed by the director of the compliance department, and the internal audit department verifies the correctness of the results.

The third level (corporate risk profile):

The profile is to be examined by the internal audit department.

24. **General rules.**

1. Employees on all levels are to study, understand and implement these procedures, and to request clarifications as they deem necessary to perform their duties.

2. Any staff member holding a managerial position at the Bank must adhere to the Bank’s policies and procedures, as well as the laws, regulations and instructions relating to anti-Money Laundering and Terrorism Financing, each according to his field of work.

3. It is prohibited for any staff member holding a managerial position to manage any accounts by proxy for any customer, except for the spouse or the first-degree relatives and after obtaining the approval of the general manager or the regional manager.

4. It is prohibited for any staff member holding a managerial position to disclose, whether directly or indirectly or by any means whatsoever, any notification made by the Unit in relation to any of the notification procedures that are known to the entity that is obliged to send a notification in accordance with the Anti-Money Laundering and Terrorism Financing Law No.(46) for the Year (2007).

5. It is not permitted to question and investigate any customer based on suspicion of Money Laundering and Terrorism Financing. This is due to that the Bank’s role in this field is limited to collecting data and information and reporting the suspicion. Furthermore, when requesting supporting information from the customer, it is not permitted to notify the customer that the
supporting information is being requested based on the instructions of the compliance department.

6. The criminal, civil, administrative and disciplinary liability on the Bank and its employees shall be precluded when they perform the duty of notification or providing information or data regarding any transactions that is suspected in good faith to be related to Money Laundering and Terrorism Financing in accordance with to the provisions of the Anti-Money Laundering and Terrorism Financing Law No.(46) for the Year (2007). An emphasis is hereby made that any notifications are to be exclusively through the compliance manager (MLRO).

7. The importance of not hesitating to contact the compliance department/ Anti-Money Laundering and Terrorism Financing Unit to inquire about cases that raise suspicion.

8. In the event of suspecting Money Laundering or Terrorism Financing or in case a customer refuses to fulfill any of the due diligence requirements and requests to close his account while having balance in the account; cash withdrawal is forbidden and the available balance is given to the customer through a certified cheque with the phrase (prohibited from withdrawal) written on it, so that it can be audit trailed.

9. Bank of Jordan has taken sufficient measures not to allow customers to perform commercial transactions on the accounts of natural persons (financial transactions related to business), and in the event the Bank verified that its individual customer are performing such transactions, the natural person is to be informed that he is to stop performing commercial transactions on his account. If the customer does not comply, his account is to be closed and the Unit is to be notified in the event there is suspicion of Money Laundering or Terrorism Financing as per the form and method approved by the Unit.

10. Bank of Jordan has taken sufficient measures to prohibit customers from performing transfers and exchanges through accounts of people not authorized to perform such operations. In the event the Bank verifies that its customers have performed such operation, a notification shall be sent to the Central Bank of Jordan in accordance with the laws and the Law on Exchange Operation in force, and the Unit is to be notified in the event there is suspicion of Money Laundering or Terrorism Financing as per the form and method approved by the Unit.
### 25. Definitions

<table>
<thead>
<tr>
<th><strong>Money Laundering</strong></th>
<th>Every act that involves acquiring, possessing, disposing of, transferring, managing, preserving, replacing, exchanging, depositing, investing, manipulating the value of, moving, concealing, disguising the source, nature, utilization, ownership, or attached rights of money whilst knowing that it was obtained by one of the crimes stipulated in article (4) of the law or any article that replaces it.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Terrorism Financing</strong></td>
<td>Performing by any means, whether direct or indirect, the collection or procurement of money with the intent of using them for a terrorist act as per the definition of terrorism in the legislation in force, or with knowledge that it will be used in whole or in part to commit a terrorist act whether the said act was actually committed or not.</td>
</tr>
<tr>
<td><strong>Terrorist Person</strong></td>
<td>Any natural person who committed, attempted, participated in, organized, directed another person, encourages, or contributed in a terrorist act, or had knowledge that a person intends to perform a terrorist act or is organizing or encouraging the performance of terrorist acts by people working for a mutual aim, regardless if this contribution is intentional or was intended only to encourage the performance of the terrorist act or with knowledge of the intentions of people to perform a terrorist act by any means, whether directly or indirectly, of his own free will and whether the terrorist act occurred or not.</td>
</tr>
<tr>
<td><strong>Terrorist Organization</strong></td>
<td>Any organization, entity, association, group, or cell consisting of two or more persons its aim is to commit or attempt to commit a terrorist act, whether the act occurred or not, as well as participating, contributing, or aiding in terrorist act, or directing, organizing or participating in terrorist acts by people working for a mutual aim so that this participation is intentional with the aim of encouraging the terrorist act, or with knowledge of the intentions of people to perform a terrorist act by any means, whether directly or indirectly, of his own free will and whether the terrorist act occurred or not.</td>
</tr>
<tr>
<td><strong>Suspicious Transaction</strong></td>
<td>Any transaction that is believed to be, with justifying reasons, related to be proceeds of one of the crimes stated in article (4) of the law or any article that replaces it.</td>
</tr>
<tr>
<td><strong>Unified List</strong></td>
<td>The list prepared and approved by the sanctions committee in relation to Al-Qaeda organization, Osama Bin Laden, the Taliban movement and all those associated with them whether entities or persons.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Banking Relationship</td>
<td>The relationship that arises between the bank and the customer and is related to the services and activities the bank provides its customers with.</td>
</tr>
<tr>
<td>Occasional Customer</td>
<td>The customer who does not have an account at the bank and is not connected with the bank with a Banking Relationship.</td>
</tr>
<tr>
<td>Beneficiary of the Transfer</td>
<td>The natural or legal person or legal arrangement specified by the person requesting the issuance of the transfer as the recipient of the requested financial transfer.</td>
</tr>
<tr>
<td>Non-profit Organization</td>
<td>Any legal person or legal arrangement or institution established in accordance with the relevant legislations, that collects or spend money for charitable, religious, cultural, educational, or social purposes, or any other similar purpose, without aiming for profit, division, or personal benefit from it activities, including international foreign branches for the Non-profit Organization and entities.</td>
</tr>
<tr>
<td>Control</td>
<td>The direct or indirect ability to exercise effective influence on another person’s actions and decisions.</td>
</tr>
<tr>
<td>Beneficial Owner</td>
<td>A natural person who is the actual benefiter, and who the business relationship is made for his benefit or on his behalf, or has full Control on a legal person or legal arrangement, or has the right to conduct legal action on behalf of either of them.</td>
</tr>
<tr>
<td>Foreign Politically Exposed Persons</td>
<td>Persons occupying or fulfilling senior public positions in a foreign country. Such as, president, prime minister, judicial or military officials, a high-ranking governmental position, a well-known politician, a leading figure in a political party, senior executives in companies owned by foreign countries, including the first-degree relatives of the said people or their business partners or any person that works on their behalf or hold authorizations issued by them.</td>
</tr>
<tr>
<td>Local Politically Exposed Persons</td>
<td>Persons occupying or fulfilling senior public positions in the Kingdom. Such as, president, prime minister, judicial or military officials, a high-ranking governmental position, a well-known politician, a leading figure in a political party, senior executives in companies owned by the Kingdom, including the first-degree relatives of the said people or their business partners or any person that works on their behalf or hold authorizations issued by them.</td>
</tr>
<tr>
<td>Shell Bank</td>
<td>A bank that has any of the following characteristics: 1. No physical presence in the country where it was established and obtained its license. Physical presence means the existence of an actual mind and management in a country. As for only having a local agent or low-level employees, this does not constitute a physical presence.</td>
</tr>
</tbody>
</table>
2. Does not keep records of its customers.
3. Is not subject to monitoring from a competent monitory authority whether in the country where it was established or in any other country.
4. The definition of a Shell Bank does not apply to a bank that does not have a permanent location as long as it is a subsidiary to a licensed bank that has physical appearance and is subject to efficient monitoring.

<table>
<thead>
<tr>
<th><strong>Shell Company</strong></th>
<th>A company that is used as a tool through which operations are passed without holding any assets or carrying out operation related to its activities, even if it registered.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Non-resident</strong></td>
<td>A natural or legal person who normally resides or is based outside the Kingdom, or who has not completed one year of residency inside the Kingdom regardless of the nationality of the person, excluding individuals who have permanent economic activities and permanent residence inside the Kingdom even their stay is intermittent.</td>
</tr>
<tr>
<td><strong>The Unit</strong></td>
<td>The Anti-Money Laundering and Terrorism Financing Unit established pursuant to the law.</td>
</tr>
<tr>
<td><strong>Money Laundering Reporting Officer (MLRO)</strong></td>
<td>A senior management official in the bank appointed for the purpose of notifying regarding Suspicious Transactions or transactions that related to Terrorism Financing or persons or entities that are listed.</td>
</tr>
<tr>
<td><strong>Senior Executive Management</strong></td>
<td>The general manager, regional manager, deputy general manager, deputy regional manager, general manager assistant, regional manager assistant, financial manager, operations manager, risk management manager, internal auditing manager, treasury manager (for investment), compliance manager, and any employee of the bank who has executive authority parallel to any of the mentioned authorities and is functionally connected to the general manager.</td>
</tr>
<tr>
<td><strong>Wire Transfer</strong></td>
<td>Any transfer that is conducted through a bank by using electronic means on behalf of the person requesting the issuance of the transfer, so that the money is sent to another bank where the person the money is transferred to is able to receive them, regardless if the person requesting the issuance of the transfer is the same person receiving it.</td>
</tr>
<tr>
<td><strong>Financial Group</strong></td>
<td>A group consisting of a parent company and any other legal person, who own controlling shares and coordinate jobs the rest of the group members to implement or monitor the group, with accordance to the core principles for effective banking supervision issued by the Basil Committee side by side with the subsidiary branches/ companies that...</td>
</tr>
<tr>
<td><strong>Financial Institution</strong></td>
<td>The legal person who pursuant to terms of establishment practices a financial activity or exceeds the activities stipulated in the banking law, including insurance companies for the purpose of these instructions.</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Subsidiary Company</strong></td>
<td>A company in which a person or group of persons, with a joint interest, possess at least (%50) of its capital, or this person or group of persons hold an effective interest therein that allows them to Control its management or general policies.</td>
</tr>
<tr>
<td><strong>Straight through Processing</strong></td>
<td>Payments that are performed electronically without the need for manual intervention.</td>
</tr>
<tr>
<td><strong>Legal Arrangements</strong></td>
<td>The relationship created by a contract between two or more parties and does not result in the creation of a legal personality such as direct Express Trusts of similar Legal Arrangements.</td>
</tr>
<tr>
<td><strong>Express Trusts</strong></td>
<td>The legal relationships created between the living or upon death (by a person or a guardian) who has placed the assets under the Control of the person or beneficiary or for a certain purpose, so that the assets are independent and not a part of the guardian’s assets, and the assets remain in the name of the guardian or another person (on behalf of the guardian).</td>
</tr>
<tr>
<td><strong>National Committee for Anti-Money Laundering and Terrorism Financing</strong></td>
<td>Jordan has formed the National Committee for Anti-Money Laundering and Terrorism Financing pursuant to the instructions and responsibilities contained in the Security Council resolution No. (1373) for the Year (2001) and the Security Council’s resolutions and other relevant resolutions.</td>
</tr>
<tr>
<td><strong>Technical Committee</strong></td>
<td>A committee formed by the National Committee for Anti-Money Laundering and Terrorism Financing that identifies the people, entities, groups or organization that must be listed in the list made and circulated by montitory authorities who in its turn circulates it to the financial authorities, professions, and non-financial businesses in order to freeze and confiscate the money and Economic Resources, and to review any requests submitted to release the frozen and confiscated money.</td>
</tr>
<tr>
<td><strong>Economic Resources</strong></td>
<td>Assets of any kind, whether tangible or intangible, movable or immovable, actual or potential, including assets that are deemed money but cannot be used to purchase any assets, products or services. Such as, lands, building, equipment, real estate, machinery, precious metals, precious stones….etc.).</td>
</tr>
</tbody>
</table>
Whistle Blow

A mechanism for sensing risks before they occur (sounding the alarm), by reporting in confidentiality and in good faith regarding all illegal activities and practices or that represent a violation of laws, regulations, instructions or safe banking practices, that may affect the bank either directly or indirectly, in order to limit them or avoid them as much as possible before they occur.


It is difficult to detect Suspicious Transaction that may be related to Money Laundering and Terrorism Financing operations and the exploitation of personal accounts for commercial purposes, exchange transaction and money transfer. However, there are indicators that can be relied on to observe and raise questions. Here below, we set out by way of an example the forms of these indicators and patterns based on the transactions or dealings:

First: Suspicious indicators for Money Laundering related transactions:

1. Cash transactions.
   1.1 Cash transactions that exceed (20,000) JODs or its equivalent in foreign currencies, cash transactions that fall below this limit and there are indicators that they are interconnected, are deemed as one transaction.
   1.2 Large cash deposits that seem unusual performed by a natural or legal person who conducts his apparent business through cheques or other payment instruments.
   1.3 A significant increase in cash deposits for a person without a clear justification, especially if these deposits were transferred from the account to a party that does not seem to have a defined and clear relationship with that person and within a short period of time.
   1.4 Depositing amounts of cash in several stages so that the value of the deposit each time if less than the limited stated in the beginning of this annex but the total of the deposited exceed the limit.
   1.5 Depositing amounts of cash in several stages so that they amount to large amounts.
   1.6 Focusing on cash withdrawals and deposits instead of using money transfers or other available tools without a clear justification.
   1.7 Trading large amounts of cash from small denominations to cash of large denominations without clear reasons.
   1.8 Unusual large cash deposits through ATMs to avoid direct contact with Bank employees, especially if these deposits are not consistent with the business and/or regular income and practices of the customer.
   1.9 The customer performing large cash transactions at several branches of the Bank or having so performed by numerous people on his behalf on the same day.
   1.10 The customer brings packed cash (sealed) from other banks and refuses to provide the Bank with his bank statements from other banks from which the amounts were withdrawn.
   1.11 Cash deposits that include forged money or nearly worn out, old money in large quantities.
1.12 The customer’s sudden and quick withdrawal of his balances without an acceptable reason or justification.

1.13 The partners, after obtaining a letter from the Bank confirming that each partner’s share of the company’s capital is deposited, withdraw the deposited amount after completing the procedures for registering the company, which may indicate that the company is a camouflage for other objectives other than those that were listed at the Companies Control Department.

1.14 The company’s accounts that are fed through deposits and transfers and followed by cash withdrawals in a manner not consistent with the nature of companies in the same sector.

2. **Accounts of individuals.**

2.1 The customer maintains several accounts and deposits cash in each of them, so that in their entirety constitute a large amount inconsistent with the nature of his work, except for customers whose nature of work requires maintaining more than one account.

2.2 The existence of accounts which the nature of the transactions performed on them do not appear to be consistent with the nature of the customer’s activities, so that they are used to receive and/or distribute large amounts for unclear purposes or purposes irrelevant to the account holder or the nature of this activities.

2.3 Maintaining accounts with several banks located within one geographical area and transferring the balances of those account to one account, and then transferring the whole collected amount outside the Kingdom.

2.4 Depositing cheques from third parties of large amounts, which cheques are endorsed to the benefit of the account holder and inconsistent with the relationship with the account holder or with the nature of his work.

2.5 Performing large cash withdrawals from previously inactive accounts or the previous withdrawals from the account were relatively of small amounts, or from an account which received unexpected large amounts from abroad.

2.6 A large number of people deposit amounts in an account without an acceptable justification.

2.7 The customer submits financial statements regarding his business that clearly differs from companies operating in the same sector.

2.8 For companies of relatively large activities to submit financial statements that are unaudited and certified from a legal auditor.

2.9 The company that accepts cheques from its customers but does not perform any large cash withdrawals from its accounts in exchange for depositing these cheques, which indicates the possibility of other sources of income.

2.10 A fundamental change has occurred in the method the customer’s account is managed in a way that is inconsistent with his data.

2.11 Accounts of companies or institutions showing minimal or inconsistent activity.

2.12 The value of the transactions being inconsistent with the information available to the Bank regarding the customer, his activities and his source of income.

2.13 The existence of several accounts at the Bank for several individuals who are not related but have common addresses, phone numbers, mailboxes, place of residency (apartment)...etc.).
2.14 Customers of high risks (politically exposed local people/ foreign) refuse to disclose their positions when opening an account at the Bank.

2.15 The insurance company does not provide documents proving that the customer has paid the installments of the insurance policy which the customer has been paid through the account of the insurance company as a result of satisfying the payment conditions under the policy.

2.16 The insurance company not providing the Bank with the contracts signed with the customers, which justify the transactions from and to the accounts of the company.

2.17 The appearance that the customer has established new Banking Relationships with a group of banks in preparation of opening a specific account at the Bank.

3. Transfers.
3.1 Abroad direct transfer of inward account deposits, whether in one or several payments.
3.2 Transfer of similar amounts (daily, weekly) the total of which are large amounts.
3.3 Executing transfers to a person that does not maintain an account with the Bank by using several different payment instruments, each of which are less than the limit stated in the instructions.
3.4 Incoming transfers with instructions to convert their values into cheques and sending them via mail to a person that does not have an account with the Bank.
3.5 Issuing transfers in large amounts to tax haven countries.
3.6 The beneficiary utilizing the value of incoming transfers in his account to purchase different monetary instruments immediately upon receipt of the value thereof for the purposes of making payments to a third party.
3.7 One of the accounts receives transfers in large amounts that this account has not previously received in such amounts, and in a manner inconsistent with the nature of the customer’s activity.
3.8 The customer frequently performs external cash transfers, using monies which the customer claims to be of foreign source.
3.9 The customer deposits bearer instruments to his account, and then transfer these instruments to a third or fourth party.
3.10 Performing a non-routine transfer within a package of routine transfers that are performed as one transfer (combined transfer).
3.11 Transferring large amounts to outside the Kingdom or receiving transfer from abroad accompanied by instructions for cash payment.
3.12 Transfers issued by the insurance company to customers, justified as against an insurance policy in which the terms of payment for the beneficiary were fulfilled.

4. Safe deposit boxes.
4.1 The Customer maintains several safe deposit boxes without a clear justification.
4.2 The widespread use of safe deposit boxes, which may indicate that the customer is likely to keep large quantities of cash in these boxes.
4.3 The customer frequently visits the safe deposit boxes before or after he makes cash deposits that are less than the limit stated in the beginning of this annex.

4.4 An increase in the customer’s visits to the safe deposit boxes in a way the seems strange when compared to his usual rate of visits.

5. **Investment related transactions.**

5.1 Purchasing securities for keeping in the safe deposit boxes at the Bank, whilst being inconsistent with the customer’s activities and financial position.

5.2 The customer’s lack of interest in the regular decisions that are to be made regarding the investment accounts such as fees or means of appropriate investment.

5.3 The customer liquidates a large financial position through a series of small cash operations.

5.4 The customer deposits cash payments or payment orders or traveler’s cheques or counter cheques with amounts less than the limit stated in the beginning of this annex, to fund the investment account.

5.5 The customer uses the investment accounts as a tool to transfer funds to foreign parties, especially to offshore jurisdictions.

5.6 Entering large amounts of money from abroad to invest in foreign currencies or securities where the size of the investment is inconsistent with the nature of the customer’s financial position.

5.7 Attempting to show financial operations in a more complex manner than required by using influential terminology such as hedging, prime bank notes, stand by commitment, contracts, arbitrage.

6. **Credit facilities.**

6.1 Applying for facilities for foreign companies or companies operating in offshore jurisdictions or facilities guaranteed by liabilities of foreign or offshore banks.

6.2 The customer suddenly repays a large debt without a clear and reasonable justification of the source of repayment.

6.3 The customer purchases the deposit certificates and later uses them as a guarantee for the repayment of facilities.

6.4 Obtaining credit facilities guaranteed by cash deposits.

6.5 Obtaining credit facilities against a foreign cash guarantee.

6.6 The customer transfers to abroad the values of facilities which were unexpectedly obtained.

6.7 The client pays a debt earlier than expected with amount larger than expected.

6.8 A request to obtain facilities against a mortgage of assets owned by a third party, where the sources of those assets is unknown to the Bank or the size of those assets is in inconsistent with the customer’s financial position.

6.9 The customer requests to obtain facilities or arranges a financing for him with a third party, where the source of the customer(s) financial contribution is unknown.

6.10 Obtaining credit facilities in return for mortgaging deposits of a company or subsidiaries aboard, especially if located in countries that known for producing/ marketing drugs.
6.11 The existence of circumstances surrounding the request for obtaining credit facilities that lead to the Bank’s rejection of granting these facilities due to doubts regarding the validity and correctness of the guarantee for these facilities.

7. **Financing business operations and documentary credits.**

7.1 A request by the customer for commercial financing, whether for export or import of basic product, the declared prices of which differ fundamentally and clearly from the prices in similar markets.

7.2 Issuing documentary credits or guarantee letters based on the customer’s request for tenders without the presence of contract for current project or for the benefit of an unusual beneficiary.

7.3 The customer changes the name of the beneficiary in the documentary credit shortly after the payment process.

7.4 The customer changes the place of payment in the documentary credit into an account in a country other than the country of the beneficiary.

7.5 The beneficiary from the documentary credit are companies owned by the customer or the shipping companies are owned by the same customer.

7.6 The amounts stated in the documentary credit documents submitted by the customer to the Bank or the customs department, are not identical to the original.

8. **International banking and financial transactions.**

8.1 Acknowledgment of the identification of a person by foreign sources located in countries known to produce/market drugs.

8.2 Developing large balances that are inconsistent with the normal size of the customer’s activities and the successive transfer to an account or accounts opened outside.

8.3 Performing bank transactions linked with foreign offshore banking units, the names of which are similar to legitimate banking institutes of a good reputation.

9. **Electronic banking services.**

9.1 The account receives several small money transfers, followed by large transfers to another country using the same method.

9.2 Depositing large payments on regular basis using a variety of means, including electronic deposit on a regular basis from countries that are known for producing/marketing drugs.

9.3 The customer requests to open an online account and refuses to provide the information necessary to complete the opening of the account, or refuse to provide information that normally entitle him to obtain services and facilities that the normal customer considers an extra advantage.

9.4 The customer uses the internet banking service to make a transfer between his accounts several times without a clear reason to do so.
10. **Customer behavior:**

The following behaviors are indicators that the customer is involved in illegal operations:

10.1 The customer who inquires at the bank regarding the records, regulations and instructions in the aim of being provided with sufficient information regarding Money Laundering operation and avoiding legal violations in this regard.

10.2 A customer who shows dissatisfaction and unwillingness to complete the procedures of a certain financial process when he is aware that they are required by the competent authorities.

10.3 A customer who behaves abnormally, such as not seizing the opportunity to obtain high interest to their account’s large balance and is ignorant of the basic facts relating to the financial process.

10.4 A customer who is moody and refuses to provide the Bank with the necessary identification documents.

10.5 The customer who is still a student and irregularly request the issuance of transfers or receives transfer or exchanges currencies in large unfamiliar amount that are inconsistent with his situation.

10.6 A customer who is controlled by another person when visiting the Bank, and the customer is unaware of what he is doing, or is of old age and is accompanied by another person who is not related to him when performing the financial transaction.

10.7 A customer who gives an amount of money or presents unjustified expensive gifts to an employee of the Bank and tries to persuade the employee not to verify the identification documents as well as other documents.

10.8 A customer who provides doubtful identification documents and refuses to provide the Bank with his personal information.

10.9 A customer who provides the Bank with a permanent address for him located outside the banking service area or outside the Kingdom.

10.10 A customer who refuses to disclose details of activities related to his work or refuses to disclose data or information or documents regarding to his institute or company.

10.11 A customer whose home phone, work or mobile phone is disconnected.

11. **Behaviors of the bank employee.**

The following behaviors are indicators that an employee of the Bank is involved in illegal operations:

11.1 The employee’s living standard and the level of his spending increases significantly and suddenly, in a manner inconsistent with his monthly income.

11.2 The employee assists in carrying out operations in which the final beneficiary or the counterparty is fully unknown.

11.3 The employee frequently bypasses the monitory procedures and uses an evasive policy during the performance of his job.

11.4 The employee exaggerates in the transparency, morals and financial sources of the customer in the reports he submits to the Bank’s management.
11.5 The employee avoids taking any leaves or holidays or frequently visits the Bank during his holidays.

11.6 The employee exploits his account and the powers granted to him or his position to perform actions that do not comply with the professional code of conduct.

11.7 The employee moves accounts belonging to the customers or his relatives by forged authorizations/ power of attorneys.

Second: Suspicious indicators for Terrorism Financing operations.

1. Indicators relating to the customer’s identification data:
   1.1 Providing misleading information that is difficult to verify.
   1.2 There is discrepancy in the information provided by the customer (place of passport issuance, place of last renewal of passport, country of residency, last country he visited).
   1.3 Presenting forged documents.
   1.4 The customer frequently changes his address of residency.
   1.5 The actual beneficiary belongs to a jurisdiction known for criminal activity or security disturbances.
   1.6 Information or indications that the customer is related to extremist people, organizations, institutions, or supports posts for extreme acts.
   1.7 Frequent change of persons authorized to dispose of a specific account or change of the actual beneficiaries.
   1.8 The employee of the Bank has knowledge that the customer has a criminal record, or it becomes known from reliable sources such as the media that the customer is involved in illegal activities.

2. Indicators relating to accounts:
   2.1 Transactions with persons/ entities with whom their relationship with the suspect is not clear.
   2.2 Dealings with multiple persons without a clear justification, especially if they are of foreign nationalities.
   2.3 Discrepancy between the nature of the customer’s activity and the method the account is managed, for example a student sending remittances.
   2.4 The customer manages several accounts with power of attorneys given to him from people whom he has no clear relationship with.
   2.5 Repeatedly using the same withdrawal voucher as a justification for the source of money when depositing them at other parties (banks), as the original of the withdrawal voucher is required to be filed and kept in the customer’s file.
   2.6 Joint accounts that are opened by two or more persons without there being a business relationship between them.
   2.7 Dormant accounts with low balances that suddenly receive deposits/ remittances (frequent) followed by daily cash withdrawals.
2.8 The account is managed by several authorized signatories without a clear connection between them.
2.9 The existence of deposits to the customer’s account although the know your customer form states that the only income was the salary transferred to the Bank.
2.10 The customer’s salary suddenly stops being transferred to the Bank without the customer requesting a clearance or his official termination.
2.11 The nature of the performed financial operations on personal accounts does not reflect normal living expenses.
2.12 Parties of the requested/ performed transaction are subject to investigation by a foreign authority or are listed on an international ban list.
2.13 The customer stops withdrawing amounts from his salary account for a relatively long period without a clear justification, which indicates the presence of another source of income.
2.14 Establishing companies and institutes that will later turn out to be Shell Companies or using their accounts in performing Suspicious Transactions.

3. **Indicators related to cash deposits.**
3.1 Cash deposits the source of which are remittances paid through exchange companies.
3.2 Cash deposits from persons who do not have a clear relationship with the account holder.
3.3 Cash deposits at branches followed by direct cash withdrawals via ATMs in locations relatively far from the location of deposit, or in locations known for gatherings of extremist groups.
3.4 Forged papers are frequently found in the customer’s deposits.
3.5 Deposit transactions that are shortly followed by remittances, especially those from/to areas of high risks.
3.6 Deposits of large amounts of cash which were brought through borders or not providing a declaration/disclosure form in relation to the possession of those amounts.

4. **Indicators related to remittances:**
4.1 Frequent or large remittances from and to countries under political or security strikes.
4.2 The customer provides illogical justification regarding incoming and outgoing remittances from other parties with whom the relationship between them is not clear (debt repayment, family aid).
4.3 Many remittances, whether local or foreign without a clear justification.
4.4 Transferring frequent or large amounts of money to persons located in places known for criminal activities.
4.5 Remittances received from one or several persons with no clear relationship with the customer.
4.6 Remittances issued by the customer to another party with who he has no clear relationship.
4.7 Incoming remittances followed by transfer orders to another party(s).
4.8 The existence of fixed payment orders (remittances) without specifying the relationship between the sender and the beneficiary.

4.9 Remittances to and from countries known to support terrorism or that have security disturbances.

4.10 Remittances of equal or close value to a number of people in different countries or to one beneficiary on several accounts.

4.11 Customer who transfers multiple amounts outside the country with instructions to pay in cash, or in the event non-residing customer receives amounts from abroad with instructions to pay in cash.

4.12 Using a number of accounts to collect money and then transfer the money to persons or commercial institutions especially if they are located in high risk areas.

5. Indicators related to credit and payment instruments.

5.1 The customer obtains credit facilities in exchange of salary transfer, where reliance is made on cash deposit for paying the installments which are settled through third party(ies).

5.2 Cash withdrawals in unusual amounts that are made through the credit cards and prepaid cards.

5.3 The salary that is guaranteeing the credit facilities granted to the customer is halted due to the resignation of the customer.

5.4 The customer requests facilities against guarantees from a bank operating outside the country, especially guarantees provided by countries who have terrorist groups or are high risk countries, without clear justifications.

5.5 The customer wishes to send ATM cards and credit cards to local or foreign addresses other than his address.

6. Safe deposit boxes.

6.1 High usage of safe deposit boxes, which may indicate that the customer keeps cash inside the box.

6.2 The customer’s behavior in being nervous before/upon entering to the location of the box or refusing to sign the visit form.

6.3 The customer who requests to enter the safe deposit boxes room and to use the box at times not during the designated hours.

6.4 The moody customer who refuses to sign the card for visiting the safe deposit box.

6.5 Refusal to present proof of identity when using the safe deposit box.

6.6 A customer who is controlled by another person when visiting the safe deposit box, and is unaware of what he is doing, or if the customer is an elderly.

6.7 A customer is or still in school and requests safe deposit boxes in a manner inconsistent with him being a student.

6.8 The customer visits the safe deposit box immediately before a cash deposit transaction or after a withdrawal transaction.
6.9 The customer authorizes a person whom he has no clear relationship to use his safe deposit box.

7. **Indicators related to charities, Non-profit Organizations, and donations:**
   7.1 The local or foreign Non-profit Organization issues and/or receives remittances from/to abroad, especially from high risk countries.
   7.2 Transfers between customer accounts and the charity’s accounts without a clear justification.
   7.3 Transactions related to humanitarian organizations that are not officially registered.
   7.4 Collecting donations in an informal or unlicensed way.

8. **Indicators related to customer behavior:**
   8.1 Signs of anxiety and nervousness on the customer or his representative during the performance of the transaction.
   8.2 The customer has reservations regarding the information he provides when opening the account or when inquiring from him on any transactions that were performed on his bank account.
   8.3 The customer’s attempt to cancel any financial (banking) transactions after knowledge that the information provided by him will be audited/ his frustration from (the procedures, systems used) at the Bank.
   8.4 The customer provides several justifications/ explanations regarding the financial transactions intended to be performed on the accounts.
   8.5 The customer’s avoidance (fear) of meeting the Bank’s employee face to face and resort to using alternative methods (ATM).
   8.6 The customer refuses to send any documents to his mail address.
   8.7 The customer resorts to choosing the employee who does not request supporting documents from the transactions intended to be performed on the account.
   8.8 Suspicion of the customer’s behavior regarding the existence of extremism ideas, such as refusal to deal with female bank employees.
   8.9 The customer’s nationality and profession do not fit with his name, appearance or beliefs.

9. **Indicators relating to employee behavior.**
   9.1 Sudden and noticeable change in the employee’s behavior, especially regarding his ideological and intellectual ideas.
   9.2 The Bank receives personal foreign remittances from high risk countries.
   9.3 Transfers from the employee’s account to customer’s accounts in the Bank with which they have no clear relationship.
   9.4 Cash deposits in the employee’s account from third parties with whom he has no clear relationship.
   9.5 The employee who shows signs of a high standard of living that is not consistent with the salary he receives.
   9.6 The appearance of transactions on the employee’s account that are inconsistent with the expected transactions.
9.7 The employee’s failure to provide the Bank with a non-conviction certificate issued by the Ministry of Justice.

10. Other indicators:
   10.1 Failure of the insurance company to provide the Bank with contracts signed with customers which justify the transactions from and to the company’s accounts.
   10.2 Life insurance policies purchased by customers of young age with no fixed income.
   10.3 Remittances issued by the insurance company to customer justified as against an insurance policy that has met the conditions of payment to the beneficiary.
   10.4 Attempt to exchange foreign currencies belonging to high risk countries and that are not used internationally.

Second: Annex on the Indicators of the exploitation of personal accounts for commercial objectives and for the purposes of exchange operations and remittances:

1. Customer accounts:
   1.1 Customer identification data indicates the customer’s practice of commercial activities.
   1.2 The size of the expected financial movements on the account according to the statements of the customer conflicts with the nature of the customer’s job and the purpose of opening the account.
   1.3 The customer requests frequent cheque books with large numbers of papers and in such a manner that does not correspond to the personal use of cheques declared by the customer.
   1.4 The main purpose of opening the account is to send and receive foreign remittances, the purpose of which is commercial remittances.
   1.5 The customer has multiple sub-accounts at one bank.
   1.6 Intensive transfers or cheque deposits from the company’s account to the account of one of its employees and vice versa.

2. Transactions performed on the accounts:
   2.1 The nature of the granted credit facilities is related to commercial activities such as capital financing (overdraft), establishing commercial complexes, trading in lands and real-estate, trading in cars...etc.
   2.2 The customer maintains a personal account and a commercial account for the company, and financial operation focus on the personal account instead of the company’s account.
   2.3 The customer’s personal account balances are low although they experience high turnover.
   2.4 The financial transactions that are performed on the account are performed with companies or individuals who Control companies.
   2.5 The account witnessing frequent financial transactions especially with the same relevant parties.
   2.6 Performing intensive financial transactions on the account on both the debtor and creditor’s side.
2.7 Granting indirect credit facilities on personal accounts in which the second party is a company, or the second party is a natural personal and the purpose for the grant is a commercial purpose such as guarantees...etc.

2.8 Internal transfers from/to the customer’s account, from/to the accounts of natural persons with the reason for the transfer being commercial.

2.9 Internal transfers from/to the customer’s accounts, from/to any company or institutes of owners of institutes or holders of companies’ accounts.

2.10 Incoming or outgoing cheques from/to the customer’s account, from/to the accounts of companies, institutes, owners of institutes or companies’ accounts.

2.11 Cheques deposited in the customer’s account from accounts of natural people with a commercial purpose.

2.12 Cheques drawn from the customer’s account to the accounts of natural persons for commercial purposes.

3. Cash transactions:

3.1 The data stated in the cash deposits form indicates the existence of a business relationship.

3.2 Intensive cash deposits accompanied by withdrawals while maintaining a low credit balance, in a manner that suggests that the customer deposits his daily income from sales into his account.

3.3 Large and frequent cash deposits into prepaid cards followed by payments to commercial parties.

3.4 Cash withdrawals for commercial purposes.

4. Credit cards:

4.1 The revolving balance in the credit card/ digital wallet frequently exceeds the credit limit by at least double.

4.2 Remittances incoming to the online shopping cards are intensive.

5. Remittances:

5.1 The data shown in the remittance form (incoming and outgoing) or its purpose indicates any commercial or business relationships or for commercial purposes such as the price of goods, paying bills, etc....

5.2 The customer receives incoming remittances or send remittances the sources of which or the recipients are companies or institutes or owners of companies/institutes.

5.3 Receiving incoming remittances from a person or a company in a foreign country and then directly transferring them to other people or company in the same country or another foreign country or to the same account of the same source in another country.

6. Electronic banking services:
6.1 The customer uses internet banking services for the transfer so that the Beneficiary of the Transfer is a company, or the customer has mentioned that the purpose of the transfer is commercial.

6.2 Transfers via e-fawateerkom.com to pay custom fees.

7. **Examples of indicators of personal accounts being abused to perform transactions related to exchange and remittance operations belonging to people unauthorized to do so:**

7.1 The existence of cash deposits and/or cheques deposited in a personal account by a person(s) related to exchange companies (partners/employees).

7.2 The existence of cash deposits and/or cheque deposits in a personal account by person(s), followed by cash withdrawals of those amounts.

7.3 The customer’s identification data contain in the sections of the field of work and/or sources of income as being from and exchange company.

7.4 Include a clause for the purpose of the transaction (exchange, currency exchange, remittance, study expenses) so that they do not commensurate with the nature of the business or the purpose of opening the account for people and/or companies unauthorized to engage in money exchange business and remittances.

7.5 The customer’s justification for some financial transactions that are performed on his account is him being an employee of an exchange company or being connected to an exchange company.

7.6 Opening several personal accounts in different currencies without a justified purpose.

7.7 The existence of several incoming remittances to a personal account from individuals and companies without a justified purpose followed by a cash withdrawal in amount approximate to the amount received into the account.

8. **Examples of parties that are not required to register in the commercial registry at the Ministry of Industry, Trade and Supply:**

<table>
<thead>
<tr>
<th>Lawyers</th>
<th>Lawyers are not required to register their law offices as they are people of a profession, unless a group of lawyers desire to register a company for themselves.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doctors</td>
<td>Doctors are not required to register their private clinics as they are people of a profession, unless a group of doctors desire to register a health center or emergency center for themselves.</td>
</tr>
</tbody>
</table>