



**GLA  
& CO**

[WWW.GLACO.COM](http://WWW.GLACO.COM)

# INTRODUCTION

On 24 December 2023, the Central Bank of Egypt ("**CBE**") issued regulatory controls for banks regarding combating money laundering and terrorist financing ("**Regulations**").

The Regulations are part of the CBE's efforts to keep pace with international standards in combating money laundering and terrorist financing, adopting best international practices in this field, and reinforcing what is already in place in practical application.

Licensed banks are granted a grace period of six 6 months from the date of issuance of the Regulations to rectify their status (i.e., by 24 June 2024).

# SCOPE OF APPLICATION

These regulations apply to all banks operating in the Arab Republic of Egypt (“Egypt”), including their branches abroad, as well as the branches of foreign banks operating in Egypt.

If the host country does not allow the proper implementation of anti-money laundering and terrorist financing measures in accordance with the requirements of Egypt, the bank – including its branches abroad and subsidiaries – must ensure the application of additional measures suitable for managing money laundering and terrorist financing risks to ensure compliance with those requirements. The bank is also required to inform the CBE of these measures.”

# GOVERNANCE

The responsibility for ensuring compliance with the requirements of anti-money laundering and terrorist financing lies with the bank's board of directors ("**Board**"). The Board is tasked with documenting its role and responsibilities, and the decisions it issues in this regard, as follows:

- ➔ Adoption of policies for combating money laundering and terrorist financing.
- ➔ Adoption of regular supervisory reports prepared regarding anti-money laundering and terrorist financing, as presented by the audit committee.
- ➔ Ensuring that the risks of money laundering and terrorist financing are accurately and comprehensively assessed to develop appropriate policies for managing those risks.
- ➔ Adoption of an acceptable level of money laundering and terrorist financing risks at the bank level as a whole, as well as business sectors, and monitoring compliance periodically as determined by the Board.
- ➔ Verification of continuous support for the compliance sector with sufficient human resources, qualified personnel, electronic systems, and appropriate tools. Also, ensuring the sector's independence and guaranteeing the confidentiality of information received regarding unusual operation reports and suspicion reports, as well as the adequacy of the measures taken to ensure the effectiveness of the application of adopted policies, procedures, and internal controls for combating money laundering and terrorist financing.

# THE MANAGER

The appointment of the responsible manager and his delegate requires banks to adhere to the following:

- The manager responsible for compliance at the bank should be the manager responsible for combating money laundering and terrorist financing, with approval from the CBE upon appointment.
- Identification of the person who will act as a delegate for the manager responsible for combating money laundering and terrorist financing during his absence.
- Notification of the CBE and the Unit with the contact details of the responsible manager and his delegate, with updates to be provided in case of any changes, termination of service, resignation, or transfer of either of them.

# ASSESSMENT OF MONEY LAUNDERING AND TERRORIST FINANCING RISKS

The bank should take appropriate measures to implement a risk-based approach by identifying, understanding, and assessing money laundering and terrorist financing risks. **The nature and scope of the risk assessment process should be proportionate to the nature and size of the bank's operations.** The risk assessment should be documented and endorsed through a report submitted to the Board, updated periodically – at least annually or as needed – after its approval by the internal audit committee.

# POLICIES, PROCEDURES & INTERNAL CONTROLS

The bank must create suitable internal policies, procedures, and controls to consistently follow anti-money laundering and terrorist financing requirements, using a risk-based approach. This should include:

- Identifying and minimizing potential risks through the bank's risk assessment process.
- Documenting and approving policies by the Board, with periodic reviews and updates at least every 2 years or as needed based on risk assessments.
- Ensuring easy access to anti-money laundering and terrorist financing policies for all relevant bank staff.
- Implementing adopted policies and procedures at foreign branches and subsidiaries.
- Ensuring that policies and procedures meet all anti-money laundering and terrorist financing requirements, including those for customer due diligence and compliance with relevant laws and instructions.



# REQUIREMENTS FOR REPORTING SUSPICIOUS ACTIVITIES

## General Requirements

The bank should not disclose, directly or indirectly, to the customer, beneficiary, or entities other than the competent authorities as per the provisions of the Anti-Money Laundering Law and its amendments, within the limits of its jurisdiction, any operations suspected to constitute proceeds of money laundering or involve money laundering or terrorism financing.

## Internal Notification Requirements

The bank is required to have procedures and systems in place for its employees to identify and report all operations suspected of involving money laundering or terrorism financing, regardless of their value. Immediate internal notification is necessary, facilitated through clear and secure channels.

Additionally, the bank should ensure the prompt examination of all internal suspicion reports and conduct periodic evaluations of its procedures and systems, taking necessary actions to enhance their effectiveness based on the evaluation results.

## Egyptian Financial Intelligence Unit Notification Requirements

The bank is required to promptly notify the Egyptian Financial Intelligence Unit (“Unit”) through its electronic system or other systems about all operations suspected of involving money laundering or terrorism financing. This notification should occur as soon as suspicions arise, and the bank must have appropriate procedures and systems in place. Additionally, the bank should adopt internal procedures compatible with the Unit’s systems, regularly assess their effectiveness, and take necessary measures for updates.

The bank should promptly provide the Unit with relevant data or information that may support or refute suspicions in previous notifications, attaching supporting documents if available. The bank should also take actions to benefit from feedback received from the Unit, improving the quality of suspicion notifications and the overall anti-money laundering and terrorism financing systems.



# THE RETENTION OF RECORDS AND DOCUMENTS

## 1 Records and documents that the bank must retain as a minimum

The bank is obliged to retain essential records and documents, including those obtained through due diligence on customers, transaction details, reports on unusual transactions, records of suspicious transactions with associated notifications, decisions on examined transactions, results of analyses, training program records for employees involved in combating money laundering and terrorism financing, and records related to screening Security Council lists and terrorist entities.

## 2 Conditions that must be followed when retaining records and documents

The bank is required to retain records and documents securely with backup copies stored in a different location. Electronic versions of the records must also be maintained noting that the same must adhere to relevant controls set by the CBE. The operation records should be comprehensive enough to reconstruct individual operations, serving as evidence against criminal activity when necessary. The process of retrieving these records and documents should be easy and prompt, ensuring the timely provision of any requested data. Additionally, the procedures and systems for record preservation should include specifications for the authorized individuals who can access these records and documents, outlining their permissions accordingly.

## 3 Retention period for records and documents

In addition to abiding by the Anti-Money Laundering Law and its executive regulations, the bank must retain records, documents, and due diligence procedure records for a minimum of 5 years after the closure of accounts or the execution of transactions for customers without accounts, unless a longer retention period is requested by the unit or investigative authorities. Specifically, for files related to unusual operations without a decision to retain, the bank must keep records, documents, and analysis results. Additionally, for files related to Security Council lists, terrorist entity lists, and local terrorists, records and documents concerning the disclosure of these lists and the outcomes of freezing and unfreezing operations for customers should be retained.



**GLA  
& CO**

[WWW.GLACO.COM](http://WWW.GLACO.COM)