COTA Commercial Bank's Policy and Procedures for the Assessment of Money Laundering and Financing of Terrorism Risks

Article 1 The Risk Policy and Procedures are formulated in accordance with the " Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated by the Financial Supervisory Commission ", the " Guidelines Governing Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program Development by the Banking Sector " of the Bankers Association of the Republic of China, the " Guidelines Governing Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program Development by the Institutions Engaging In Credit Card Business " and the " Guidelines Governing Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program Development by the Trust Enterprises" of the Trust Association of the Republic of China. The content covers aspects such as how the bank recognize and assess risks of money laundering and financing of terrorist in businesses, and development of a program on anti-money laundering and combating the financing of terrorism, etc. as the basis for implementation.

Article 2 The Bank's internal control system shall be approved by the Board of Directors and, if amended, the same shall apply. The risk control mechanism or the internal control system of a bank should include identification, evaluation, management carried out for risks of money laundering and financing of terrorism, relevant written policies and procedures setup, and programs set up in accordance with the results of risk assessments to prevent money laundering and combat the financing of terrorism and routine review shall be conducted.
A risk-based approach is designed to help the development of prevention and reduction measures corresponding to money laundering and financing of terrorism in order for the bank to determine its allocation of resources for anti-money laundering and combating the financing of terrorism, establish its internal control system, and formulate and implement policies, procedures and control measures which should be taken for programs to prevent money laundering and combat the financing of terrorism.
The bank has a diversity of businesses, such as consumer banking, corporate banking, investment services (or wealth management), credit card, trust (such as money trust, securities trust , real estate trust, and so forth), cross-border correspondent banking, with which risks of money laundering and financing of terrorism associated are also different in each banking business. The bank shall take above differences in banking businesses when assessing and reducing its risk exposures against money laundering and financing of terrorism.

Article 3 The bank shall conduct appropriate measures to identify and evaluate its risks of money laundering and financing of terrorism, and formulate specific risk assessment projects based

on the risk identified to further control, reduce or prevent the risk. Specific risk assessment projects should at least include indicators such as geography, customer and product, and transaction and payment channel and a further analysis for each risk project should be conducted to formulate the details of risk factors.

(1) Geographical risk:

i. The bank should identify regions with higher risk of money laundering and financing of terrorism.

ii. When formulating a list of regions with higher risks of money laundering and financing of terrorism, the bank may select applicable references based on practical experience of its respective branch.

(2) Customer risk:

i. The bank shall take comprehensive consideration of an individual customer's background, occupation and characteristics of socioeconomic activities, region, organizational pattern and structure of a non-natural person customer in order to identify risks of money laundering and financing of terrorism from the customer.

ii. In identifying individual customer risks and determining their risk level, the following risk factors are used as the basis for assessment:

1. Geographical risk of the customer: Determine the risk rating of the customer's nationality and country of residence based on the list of regions with risks of money laundering and financing of terrorism defined by banks.
2. Money laundering risk of the customer's occupation and industry: Determine the risk rating of the customer's occupation and industry based on money laundering risk of occupations and industries defined by banks. High-risk industries such as businesses engaged in intensive cash transactions, or firms or trusts easily applied to hold individual assets.
3. Name of company/organization by where the customer works.
4. The channel where the customer opened accounts, signed contracts and built business relationships.
5. The amount of initial business relationship transactions.
6. The product or service requested by the customer.
7. Whether the customer has characteristics of other high-risk money laundering and financing of terrorism; for example, the customer is unable to make reasonable explanations when the address left too far from the branch, the customer is a company with anonymous shareholders or being able to issue unregistered stocks, or the equity complexity of a corporate customer, such as whether the shareholding structure is obvious unusual or overly complex relative to its nature of business.

(3) Product, service, transaction, and payment channel risk

i. The Bank should identify those who may pose a higher risk of money laundering and financing of terrorism based on the nature of individual products and services,

transactions or payment channels.

ii. Before launching new products or services or conducting new business (including new payment mechanisms, use of new technology in existing or new products or business), banks should conduct risk assessment of money laundering and terrorist financing and establish corresponding risk management measures to reduce the identified risks.

iii. The risk factors for individual products and services, transactions or payment channels are as follows:

1. The extent of the relationship with cash.
2. The channel through which the business relationship or transaction is established, including whether it is a face-to-face transaction and whether it is a new payment instrument such as electronic banking.
3. Whether the transaction is a high-value transfer of money or value.
4. Anonymous transactions.
5. Receipt of funds from unknown or unrelated third parties.

Article 4 The Bank shall consider the relevant risk factors and classify the risk level of customers into three risk levels, namely high risk, medium risk and low risk, as a basis for the Bank to strengthen its customer screening measures and continuous monitoring mechanism. The bank is not allowed to disclose the information about the risk rating of a customer to its customers or persons unrelated to obligations of implementing ant-money laundering.

Article 5 The following customers should be classified as high-risk:

(1) PEP in foreign governments

(2) Terrorists or groups that are subject to economic sanctions, identified or investigated by foreign governments or international money laundering prevention organizations, and individuals, legal persons or groups that are sanctioned under the Prevention of Terrorism Act.

(3) The bank may, base on its own business type and consideration of associated risk factors, formulate types of customers which should be directly classified as high-risk customers.

The Bank may define the type of customer that can be directly classified as low risk based on a complete written risk analysis that adequately describes the type of customer commensurate with the lower risk factors.

Article 6 For customers to establish new business relations, the bank shall determine their risk ratings when establishing business relations.

For existing customers with identified risk ratings, the bank shall conduct a risk reassessment of customers based on its policies and procedures to assess risks.

The Bank reassesses customer risk and adjusts the customer risk level in due course at the

following points in time:

(1) When a customer opens an additional account, when a supplemental contract for trust business has a significant impact, or when a new business relationship is created.

(2) When conducting a regular review of a customer according to risk ratings of a customer.

(3) When the Bank learns of a significant change in the identity and background information of a customer.

(4) When an event occurs that may result in a material change in the risk profile of a customer, such as a reported suspicion of money laundering or terrorist transaction.

The Bank shall regularly review the adequacy of the information it obtains to identify customers and actual beneficiaries and ensure that such information is updated, especially for high-risk customers, at least once a year.

Article 7 The bank shall establish the corresponding control measures according to identified risks to reduce or prevent risks of money laundering. The bank shall determine different control measures applicable to customers with different risk ratings based on risk profiles of customers.

(1) For high-risk customers and customers with specific high-risk factors, the following control measures may be applied:

i. Enhanced Due Diligence

1. To obtain information related to the purpose of the account opening or trust business contract and transactions: expected account usage (e.g., amount, purpose and frequency of expected transactions).
2. To obtain information on the source of wealth, the source and destination of funds, and the type and amount of assets of individual customers. If the source of funds is a deposit, further information on the source of the deposit should be obtained.
3. To obtain further business information from corporate customers, group customers or trustee customers: to understand the latest financial status, business activities and business transactions of customers in order to establish their assets, sources and destination of funds.
4. To obtain descriptions and information about upcoming or completed transactions.
5. To conduct on-site or telephone interviews according to the customer type to confirm the actual operation of the customer.

ii. Approval of senior management (branch general manager) should be obtained prior to establishing business relationship with customer.

iii. Increase the frequency of CDD, and conduct CDD at least once a year.

iv. Enhance the monitoring mechanism

(2) For medium-risk customers, the following control measures may be applied:
   i. EDD and transaction screening
   ii. Approval of supervisor should be obtained prior to establishing business relationship with customer.
   iii. CDD at least every three years.

(3) For low-risk customers, the following control measures may be applied:
   i. Approval of AVP should be obtained prior to establishing business relationship with customer.
   ii. CDD at least every five years.

Except for the cases in Article 6 (1) (3) of the "COTA Bank Guidelines Governing Anti-Money Laundering and Combating the Financing of Terrorism", the Bank shall adopt simplified measures for lower risk cases in accordance with its risk prevention policies and procedures. Such simplified measures shall be equivalent to the lower risk factors and the simplified measures may be adopted as follows:

(1) Reduce the frequency of updating customer identification information.
(2) Reduce the degree of continuous monitoring, and use a reasonable threshold amount as a basis for reviewing transactions.
(3) If the purpose and nature can be deduced from the transaction type or the established business relationship, gathering specific information or performing special measures will not be necessary to understand the purpose and nature of the business relationship.

Article 8 The Bank shall establish regular comprehensive money laundering and financing of terrorism risk assessments and produce risk assessment reports to enable management to understand the overall money laundering and financing of terrorism risks in a timely and effective manner, determine the mechanisms to be put in place and develop appropriate mitigating measures. The Bank shall conduct a comprehensive biennially money laundering and terrorism risk assessment exercise based on the following indicators:

(1) The nature, scale, diversity and complexity of businesses
(2) Target market
(3) Number and scale of banking transactions: Consider general transaction activities of the bank and characteristics of its customers
(4) Management data and reports associated with high risks: such as the number and proportion of high-risk customers, the amount, quantity or proportion of high-risk products, services or transactions, the nationality, place of registration or place of business, the amount or proportion of transactions involving high-risk areas, etc.
(5) Business and products, including the channel and manner to provide services and products to customers, the way to implement the customer review measures, such as the

extent to use of information systems, whether the third person is entrusted to perform the review, etc.

(6) The inspected results from internal audit and the supervisory authority.

When the bank conducts a comprehensive risk assessment of money laundering and financing of terrorism, in addition to considering the above indicators, the information obtained from other internal and external sources is recommended as supporting information. For example:

(1) The management reports provided by the bank's internal management (such as supervisors of business units, or relationship managers of customers, etc.).

(2) Relevant reports released by international organizations and other countries for prevention of money laundering and combating financing of terrorism.

(3) Information released by the Competent Authorities on risks of money laundering and financing of terrorism.

The results of the bank's comprehensive risk assessment of money laundering and financing of terrorism should be used as a basis for the development of a program on anti-money laundering and combating the financing of terrorism. The bank should allocate adequate personnel and resources based on the results of risks assessment and take effective countermeasures to prevent or reduce risks.

With any major change in the bank itself, such as the occurrence of major events, major development of management and operation, or the happening of new relevant threats, the assessment should be re-conducted.

When the risk assessment report is completed or updated, the risk assessment report should be sent to the FSC for review.

Article 9 In order to prevent money laundering and terrorist financing related crimes, the Bank shall establish a policy of continuous monitoring of accounts and transactions by checking the names of customers and transaction related parties and identifying suspicious transactions with suspected money laundering or terrorism financing patterns. Such control policies and procedures shall be approved by the President.

Article 10 The international department of the Bank shall establish policies and procedures for risk assessment, review and control mechanisms when conducting correspondent banking and other similar business. Such policies and procedures shall be approved by the President.

Article 11 If there are any other outstanding matters, they will be dealt with in accordance with the decrees of the competent authorities. Such rule shall be approved by the President.

Article 12 This Risk Policy and Procedures will be revised following the update of " Guidelines Governing Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention

Program Development by the Banking Sector ", " Guidelines Governing Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program Development by the Trust Enterprises " and " Guidelines Governing Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program Development by the Institutions Engaging In Credit Card Business" and will be implemented upon endorsement by the AML/CFT Committee and approval by the Board of Directors; the same shall apply to any amendment thereto.