Annex

"Guidelines for Banks Regarding Assessment of Money Laundering and Terrorism Financing Risks and Adoption of Prevention Programs"

Financial Supervisory Commission dated May 11, 2015
Jin-Guan-Yin-Fa-Zi No. 10400092790 Letter approval for recordation
Financial Supervisory Commission dated June 28, 2017
Jin-Guan-Yin-Fa-Zi No. 10610003210 Letter approval for recordation
Financial Supervisory Commission dated April 23, 2019
Jin-Guan-Yin-Fa-Zi No. 10801049540 Letter approval for recordation

I. These Guidelines are established in accordance with "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" for the purpose of anti-money laundering and countering terrorism financing (AML/CFT) to cover how banks identify and assess money laundering and terrorist financing (ML/TF) risk in businesses and establish AML/CFT programs, etc., as a basis for implementation.

II. A bank's internal control system and its amendment should be approved by the Board of Directors. In addition, the internal control system should include relevant written policies and procedures for identifying, assessing and managing ML/TF risks, AML/CFT programs based on risk assessment results, and the periodic review of such policies, procedures and programs.

The purpose of a risk-based approach is to help a bank develop prevention and mitigation measures that are commensurate with the ML/TF risks identified, determine the allocation of resources on AML/CFT, establish internal control system, and establish and implement policies, procedures and measures that are necessary in AML/CFT programs.

Banking businesses, such as consumer banking, corporate banking, investment services (or wealth management), and correspondent banking, etc., are

diversified. Therefore the ML/TF risks associated with each business are different. A bank should take such business diversity into account when assessing and mitigating ML/TF risks.

The examples provided in the Guidelines are not mandatory requirements. A bank's risk assessment mechanism should be commensurate with its business nature and scale. For a bank that is relatively small or has relatively simple businesses, a simple risk assessment is sufficient. For a bank that provides relatively complex products and services, has multiple branches (or subsidiaries) providing diversified products, or has diversified customer groups, however, is required to perform a relatively sophisticated risk assessment.

III. A banks should take appropriate measures to identify and assess its ML/TF risks, and determine specific risk categories based on the risk identified, in order to further control, mitigate or prevent such risks.

Such specific risk category should cover at least geographic areas, customers, and products, services, transactions or delivery channels, etc. A bank should further analyze each risk category to determine detailed risk factors.

(I) Geographic risk:

1. A bank should identify geographic areas that are exposed to higher ML/TF risks.
2. When building up a list of high-risk areas, a bank may determine appropriate risk factors based on the practices of branches (or subsidiaries) and its needs.

(II) Customer risk:

1. A bank should take an overall account of a customer's background, occupation, characteristics of social and economic activities, geographic areas, and an entity customer's organization type and structure, etc., to identify the customer's ML/TF risks.
2. When identifying a customer's risk and determine the customer's level

of risk, a bank may perform risk assessment based on following risk factors:

(1) Geographic risk of the customer: Determine the level of risk of the customer's nationality and country of residence based on a list of areas that are exposed to ML/TF risks defined by the bank.

(2) Occupation and industry risk of the customer: Determine the level of risk of the customer's occupation and industry based on a list of occupations and industries that are exposed to money laundering risks defined by the bank. High-risk industries include, for example, cash-intensive businesses, or companies or trusts that tend to be used as personal asset-holding vehicles, etc.

(3) Individual customer's employer.

(4) The channel used by the customer to open account and establish business relation.

(5) The transaction amount with which the customer first establishes business relation.

(6) Products or services that the customer applies.

(7) Whether the customer has other high ML/TF risk characteristics. For example, the customer fails to provide a reasonable explanation regarding the significant geographic distance between the customer and the branch; the customer has nominee shareholders or shares in bearer form; the extent of complexity in an entity customer's ownership structure, such as whether the ownership structure is apparently unusual or excessively complex given the nature of the customer's business.

(III) Product, service, transaction or delivery channel risk:

1. A bank should identify products, services, transactions or delivery channels that have higher ML/TF risk based on the nature of individual product, service, transaction or delivery channel.

2. A bank should, before launching a new product, service or business (including new delivery mechanisms, applying new technology on existing or new product or service), perform ML/TF risk assessment and establish relevant risk management measures to mitigate the risks identified.
3. Examples of individual product, service, transaction or delivery channel risk factors are as follows:
   (1) The extent of associating with cash.
   (2) The channel to establish business relation or process transaction, including whether it allows non-face-to-face transactions, and whether it is a new delivery mechanism such as electronic banking.
   (3) Whether it allows high amount of money or value transfer.
   (4) Anonymous transactions.
   (5) Payment received from unknown or un-associated third parties.

IV. A bank should establish multiple levels of customer risk and rules to determine the level of customer risk.

Customer risk should have at least two levels, “high-risk” and “general risk”, as bases to determine the extent of customer due diligence and ongoing monitoring. For a bank that adopts only two risk levels, the bank should not take simplified measures to a customer rated as “general risk” because “general risk” is still higher than “low risk” provided in Paragraph V and VII of the Guidelines.

A bank should not disclose a customer’s level of risk to the customer or any person that is unrelated to AML/CFT obligations.

V. A bank should directly treat foreign political exposed persons, terrorists or terrorist groups that are sanctioned, identified or investigated by foreign governments or international AML organizations, and designated individuals or

entities sanctioned under Counter-Terrorism Financing Act as high-risk customers. In addition, a bank may determine the types of customers that should be directly treated as high-risk customers based on its business type and relevant risk factors.

A bank may, based on the results of an overall written risk analysis, define the types of customers that can be treated as low-risk customers. The results of the written risk analysis should be sufficient to explain that such types of customers are commensurate with lower risk factors.

VI. With respect to a new customer to establish business relation with a bank, a bank should determine the customer's level of risk when establishing business relation.

With respect to an existing customer with a specific level of risk, a bank should re-assess customer risk in accordance with its risk assessment policies and procedures.

Although a bank performs customer risk assessment when establishing business relation with a customer, for certain customers, the overall risk profile become clear after the customers use accounts to transact. Therefore, a bank should conduct due diligence to existing customers on the basis of materiality and risk, and, at appropriate times, review the existing business relationships and adjust the level of risk after taking into account the time and information sufficiency of last due diligence. Such appropriate times should at least include:

(I) When the customer opens a new account or establishes a new business relation.

(II) Time to conduct periodic review determined on the basis of the customer's materiality and risk.

(III) When a bank knows a material change occurs in the customer's identification and background information.

(IV) When the bank reports transactions suspected to involve money

laundering or terrorism financing or other events that may result in substantial change in customer risk profile occur.

A bank should review periodically the sufficiency of the information for identifying customers and beneficial owners, and ensure the update of such information. Especially, high-risk customers should be reviewed at least annually by the bank.

VII. A bank should establish control measures according to the risks identified to mitigate or prevent such money laundering risk. A bank should determine appropriate control measures according to a customer's level of risk.

With respect to such control measures, a bank should take different measures to a high-risk customer and a customer with a specific high-risk factor to effectively manage and mitigate identified risks. Following are examples:

(I) Conduct enhanced due diligence, such as:

1. Obtaining relevant information on the purpose of an account or relationship: the expected use of the account (for example, the amount, purpose and frequency of expected transactions)
2. Obtaining information on an individual customer's source of wealth, source and destination of funds, and types and quantities of assets, etc. If the source of funds is deposit, a bank should further understand the source of such deposit.
3. Obtaining an entity customer's further business information: understand the customer's latest financial situation, commercial activities and business relationship information to establish the source of assets, source of funds and destination of funds.
4. Obtaining information on the reason for intended or performed transactions.
5. Conducting site visit or phone interview, according to customer type, to validate a customer's operation situation.

(II) Obtain the approval of senior management, defined by the bank considering internal risks, before first establishing a business relation or establishing a new business relation.

(III) Increase the frequency of customer due diligence.

(IV) Conducting enhanced ongoing monitoring of the business relationship.

Except in the situation described in Subparagraph 1 of Paragraph 3 of Article 6 of the Model Guidelines, a bank may take simplified measures in a lower risk situation in accordance with its risk prevention policies and procedures. Such simplified measures should be commensurate with the lower-risk factors. Examples of simplified measures that may be applied include:

(I) Lower the frequency of updating customer identification data.

(II) Lower the extent to which the bank conducts ongoing monitoring, and review transactions that reach a reasonable amount.

(III) Exempting from collecting specific information or conducting specific measures as to the purpose and nature of business relations if a bank may infer this from the type of transactions or business relations.

VIII. A bank should establish a mechanism of periodic enterprise-wide ML/TF risk assessment and generate a risk assessment report to enable senior management to timely and effectively understand the bank's overall ML/TF risks, determine necessary mechanisms to be established, and develop appropriate mitigation measures.

A bank should establish a mechanism of periodic enterprise-wide ML/TF risks assessment based on following risk factors:

(I) The nature, scale, diversity and complexity of businesses.

(II) Target markets.

(III) Volumes and sizes of bank transactions: considering the usual transaction activities of the bank and characteristics of its customers.

(IV) Management data and reports related to high risk: such as the number

and proportion of high-risk customers; the amount, volume or proportion of high-risk products, services or transactions; the amount or proportion of customer's nationality, place of registration or operation, or transactions that involve high-risk areas.

(V) Businesses and products, including the channels and manners that a bank uses to provides customers businesses and products, and the way to conduct customer due diligence, such as the extent of using information system and whether relying on third parties to perform due diligence.

(VI) The examination results of internal auditors and supervisory authorities.

When a bank performs the enterprise-wide ML/TF risk assessment described in last paragraph, in addition to taking into account such risk factors, it is suggested to supplement the assessment with other information obtained from internal or external sources, such as:

(I) Management reports provided by the bank's management (such as head of business unit, relationship managers, etc.)

(II) Relevant AML/CFT reports published by international anti-money laundering organizations and other countries.

(III) Information of ML/TF risk released by the Competent Authorities.

A bank's enterprise-wide ML/TF risk assessment results should be used as a basis to develop AML/CFT programs. A bank should allocate appropriate headcounts and resources based on such results and take effective countermeasures to prevent or mitigate risks.

If a material change occurs to a bank, such as a material incident, material development in management and operation, or relevant new threats, a bank should re-perform the assessment.

A bank should file the risk assessment report to Financial Supervisory Commission when it is completed or updated.