King's Town Bank Anti-Money Laundering and Countering Terrorism Financing Risk Identification and Assessment Procedure

Article 1:

The King's Town Bank Anti-Money Laundering and Countering Terrorism Financing Risk Identification and Assessment Procedure is established for the purpose of anti-money laundering and countering terrorism financing pursuant to the "Regulations Governing Anti-Money Laundering of Financial Institutions," "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 "Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures" amended by Bankers Association of the Republic of China (hereinafter "the Bankers Association") according to Letter Quan-Yi-Zi No. 1080003139 dated May 31, 2019, and the "Guidelines Governing Money Laundering and Terrorist Financing Risk Assessment and Relevant Prevention Program Development by the Banking Sector" formulated by the Bankers Association.

Article 2:

The Bank shall adopt appropriate measures to identify, assess, and manage its money laundering, terrorist financing, and weapons of mass destruction (WMD) proliferation financing risks and formulate specific risk assessment items and mechanisms based on the identified risks. For high-risk customers, the Bank adopts enhanced high-risk assessment procedures. For low-risk customers, the Bank shall adopt simplified measures to allocate resources more efficiently to further control, reduce, or prevent risks. The Bank shall formulate an Anti-Money Laundering and Countering Terrorism Financing Plan according to the risk assessment results and business scale and regularly evaluate, review, and update the Plan.

Article 3:

The Bank's risk assessment items include the following aspects: geography, customers, products and services, and transaction or payment channels. The Bank shall further analyze each risk item to establish detailed risk factors to facilitate the identification and establishment of customer risk levels and grading rules.

I. Geographical risks:

The Bank shall establish and maintain a high-risk country list by referring to the following channels to identify countries/regions with high money laundering, terrorist financing, and WMD proliferation financing risks:

(I) An official notice from the Financial Action Task Force (FATF) forwarded by the Financial Supervisory Commission (FSC) to identify countries or regions with serious deficiencies in anti-money laundering and countering terrorist financing, as well as other

countries or regions that have not followed or not fully complied with the FATF's recommendations.

(II) Countries or regions that are subject to United Nations, United States, or European Union economic sanctions or other similar measures.

(III) Countries or regions listed by Transparency International's Corruption Perception Index as having a significant level of corruption.

(IV) Countries or regions identified by the International Monetary Fund (IMF) as offshore financial centers (OFCs).

(V) Countries or regions and tax havens identified in the National Risk Assessment Report as the main sources and destinations of criminal proceeds.

II. Customer risks:

(I) Perform a comprehensive consideration of individual customers' backgrounds, occupations, socio-economic activity characteristics, regions, and organizational types and structures of non-natural persons to identify money laundering, terrorist financing, and WMD proliferation financing risks.

(II) The Bank shall adopt the following risk factors as the basis for assessment when identifying the risks of individual customers and determining their risk levels:

1. Customer geographic risk: The risk rating of the customer's nationality and country of residence shall be determined according to the list of countries and regions defined by the bank for the risk of money laundering, terrorist financing, and WMD proliferation financing.
2. Customer occupation and industry-related money laundering risk: The risk rating of the customer's occupation and industry shall be determined based on the Bank's definition of the risks associated with money laundering. High-risk industries include businesses that engage in intensive cash transactions or companies or trusts that are easily used to hold personal assets.
3. Customer account opening and business relationship establishment channels.
4. Products or services applied for.
5. Is the customer unable to provide a reasonable explanation for why their registered address is too far away from the branch?
6. Is the customer a company with dormant shareholders or a company that can issue bearer stocks, or is the equity the legal person customer complex?
7. Are the customer's transactions obviously abnormal, such as those reported as suspected money laundering, terrorist financing transactions, or deposit watch-listed account?
8. Is the client or related person suspected of involvement in a special major case that is being reported by the media in real-time?
9. The Bank has determined the types of customers that should be directly considered

as high-risk based on its own business model and risk factor considerations, as shown in the appendix.

III. Product and service, transaction, or payment channel risk:

The Bank shall identify those who may pose a higher risk of money laundering, terrorist financing, and WMD proliferation financing based on the nature of individual products and services, transactions, or payment channels.

(I) A money laundering, terrorist financing, and WMD proliferation financing risk assessment must be conducted before launching new products or services or engaging in new types of business (new payment mechanisms, applying new technologies to existing or brand-new products or businesses, etc.), and the corresponding risk management measures shall be established to reduce the identified risks.

(II) Examples of individual product and service, transaction, or payment channel risk factors are as follows:

1. The degree of association with cash.
2. The channel for establishing business relationships or transactions, including whether it is a face-to-face transaction or a new type of payment tool such as electronic banking.
3. Is it a high-value money or value transfer business?
4. Anonymous transactions.
5. Payments are received from unknown or unrelated third parties.
6. Target customer groups.

Article 4:

The Bank has established different customer risk levels and classification provisions:

Customers are categorized into three risk levels: “high risk”, “general risk” and “low risk”. These categories are used to determine the necessary measures for strengthening customer due diligence and the level of implementation required for the continuous monitoring mechanism.

No bank employee may disclose customer risk level information to customers or anyone who is not involved in the implementation of anti-money laundering and countering terrorism financing obligations.

Article 5:

The Bank’s timing in identifying and assessing the risks of individual customers:

I. When establishing new business relationships or signing trust contracts, the customer’s risk level must be determined at the time of account opening or contract signing.

II. For existing customers whose risk level has been determined, the customer risk identification and assessment shall be performed again according to the risk identification and assessment method in Article 6.

Article 6:

Although the Bank has conducted risk assessments on customers when establishing business

relationships, for some customers, their overall risk profile will not become clear until they start transacting through their accounts. Therefore, the Bank shall review the identity information of existing customers based on their importance and risk level, conduct reviews of existing relationships, and adjust risk levels as appropriate after considering the timing of the previous review and the adequacy of the information obtained. The preceding appropriate timing shall at least include the following:

I. When a customer opens an additional account, adds a trust deed, or adds a new business relationship.

II. Regular customer review intervals shall be determined based on the customer's importance and risk level.

III. When significant changes in the customer's identity and background information are discovered.

IV. When an event that may lead to a substantial change in the customer's risk profile has occurred, such as suspected money laundering or terrorist financing transactions.

The Bank regularly reviews whether the information obtained on the identity of the identified customers and beneficial owners is sufficient and ensures that such information is updated. Unless otherwise provided in this Procedure, high-risk customers shall be reviewed at least once a year.

Article 7:

The Bank has established corresponding control measures based on the identified risks to reduce or prevent the money laundering risks. The Bank shall determine the control measures applicable to customers at different risk levels based on the customers' risk levels.

I. The following control measures are taken for high-risk customers to manage and reduce known risks effectively. The examples are listed as follows:
   (I) Implement enhanced customer due diligence measures.
   (II) Obtain consent from the AML/CFT supervisor before establishing or adding new business relationships.
   (III) Conduct customer due diligence at least once a year.
   (IV) Implement enhanced and ongoing business relationship supervision.

II. The following control measures are adopted for "general risk" customers to manage and reduce known risks effectively.
   (I) Conduct regular customer due diligence once every three years.
   (II) Adjust the information required for customer due diligence and reduce the number of documents or information collected from customers while complying with regulatory requirements.

III. For customers who are considered "low-risk", adopt the customer identity verification control measures listed below.
   (I) Conduct periodic customer due diligence once every seven years.

(II) If the purpose and nature of a business relationship can be inferred from the type of transaction or the existing business relationship, it is unnecessary to collect specific information or implement special measures to understand the purpose and nature of the business relationship.

IV. The Bank's Simplified Measures for Customer Identity Verification Control

(I) The preceding customer identity verification control measures need not be implemented for customers who have not had any transactions for over 12 months since opening an account at this bank (calculated from the date of the last change in their account) and whose average account balance in the past six months is within the following amount range.

1. High-risk customers: NT$30,000 (inclusive) or less;
2. General-risk customers: NT$50,000 (inclusive) or less;
3. Low-risk customers: NT$100,000 (inclusive) or less.

(II) If a dormant customer suddenly starts transacting again, or if there is a significant change in their transaction pattern (such as a sudden large transaction), the Bank shall initiate a periodic due diligence and update of the customer's risk assessment information the following month.

(III) However, the preceding simplified customer identity verification control measures shall not be adopted in the following circumstances:

1. Customers from high-risk countries or regions that do not have effective anti-money laundering or counter-terrorism financing measures in place including, but not limited to, countries or regions where an official notice from the FATF was forwarded by the FSC to identify countries or regions with serious deficiencies in anti-money laundering and countering terrorist financing, as well as other countries or regions that have not followed or not fully complied with the FATF's recommendations.
2. There is sufficient reason to suspect that the customer or transaction is involved in money laundering or terrorist financing.

Article 8:

The Bank has established a comprehensive process to assess the risks of money laundering, terrorist financing, and WMD proliferation financing and generated a report on risk assessment. These efforts can help the management to understand the overall money laundering and terrorist financing risks faced by the Bank in a timely and effective manner, decide on the mechanisms to be established, and develop appropriate mitigation measures. The Bank has established a regular and comprehensive money laundering, terrorist financing, and WMD proliferation financing assessment process based on the following indicators:

I. The nature, size, diversity and complexity of the businesses.

II. Target market.

III. Number and scale of bank transactions.

IV. High-risk related management data and reports shall include: the number and proportion of high-risk customers; the amount, quantity, or proportion of high-risk products, services, or transactions; the customer's nationality, registered place or business place; or the amount or proportion of transactions involving high-risk regions.

V. Business and products, including the channels and methods for providing business and products to customers.

VI. Internal audit and inspection results of regulatory authorities.

VII. Management reports provided by the Bank's internal management.

VIII. Anti-Money Laundering and Countering Terrorism Financing-related reports issued by the FATF and other countries.

IX. Money laundering, terrorist financing, and WMD proliferation financing risk information published by supervisory authorities.

The comprehensive money laundering, terrorist financing, and WMD proliferation financing risk assessment results of this Bank shall serve as the basis for the development of the Anti-Money Laundering and Countering Terrorism Financing Plan. This bank will allocate appropriate workforce and resources to implement effective risk prevention or reduction measures based on the risk assessment results.

The Bank must implement the assessment operations again when it encountered major changes such as severe incidents, significant developments in management and operations, or relevant new threats have been discovered.

The Bank shall submit the risk assessment report to the FSC for reference when the risk assessment report is completed or updated.

Article 9:

This Procedure shall be implemented after approval by the board of directors. The same shall apply to its amendments. However, the authorization to amend only the appendix shall be approved by the general manager.

Formulated 11-23-2015
Amended 01-01-2017
Amended 09-11-2017
Amended 08-20-2018
Amended 07-29-2019
Amended 10-12-2020
Amended 02-21-2022
Amended 02-20-2023
Amended 12-25-2023