Suggested Best practices of Comprehensive Assessments of Risks Related to Money Laundering and Terrorism Financing in Banks

I. Background

The comprehensive risk assessments for money laundering and terrorism financing, refers to a mechanism to review the residual risks of banks by identifying the general and specific money laundering (ML) and terrorism-financing (TF) risks faced, and assessing the related risk control measures of banks, so that appropriate actions may be taken to manage the ML and TF risks effectively.

The outcomes of the comprehensive risk assessments for money laundering and terrorism financing help banks to assess if their resource allocations and controls measures are appropriate, or if there is any need for adjustment. It also corresponds to the 40 recommendations launched by FATF in 2012, which addresses the importance of a risk-based approach to AML/CFT tasks with limited resources.

With regard to their comprehensive risk assessments for money laundering and terrorism financing, banks shall adhere to the rules and regulations of "Directions Governing Internal Control System of Anti-Money Laundering and Combating the Financing of Terrorism of Banking Business, Electronic Payment Institutions and Electronic Stored Value Card Issuers" by the Financial Supervisory Commission (FSC), and the "Template of Important Notes for Anti-Money Laundering and Combating the Financing of Terrorism to Banks," and its appendix "Guidelines for Banks Assessing Anti-Money Laundering and Combating the Financing of Terrorism Risk and Countering Planning," by BAROC.

This document aims to help banks' operations regarding identifying, assessing, and implementing their comprehensive risk assessments for money laundering and terrorism financing, and to provide descriptions of practical executions and approaches, as references to our members. This is not the self-regulations established by BAROC, and thus not binding in any way. The member banks may proceed with their own risk assessments and prepare the risk assessment report according to the characteristics of their operations, risk levels, and group policies, while adhering to the current related laws and regulations of anti-ML and counter TF.

This document also provides the methodologies and outcomes of the National Risk Assessment (NRA) and the Sectoral Risk Assessment (SRA), as an incorporated reference of the comprehensive risk assessments for money laundering and terrorism financing for banks.

II. The Descriptions of the Principles of the comprehensive risk assessments for Money Laundering and Terrorism Financing

(I) There are various methodologies to implement the comprehensive risk assessments for money laundering and terrorism financing. When applying these risk assessments, the banks shall adopt the most suitable methodology according to their nature, scale, diversification, complexity, degree of globalization, among other things. There is not one single methodology for all the banks.

If there are other businesses operated by the banks, these side businesses shall be also included in the scope of the comprehensive risk assessments for money laundering and terrorism financing, providing the methodology shall be specific to the bank in question. It is not necessary to have one single side business as the subject of the assessment, nor to prepare an assessment report for one single side business.

(II) With regard to small or simple banks, a simplified risk assessment is sufficient. However, for institutions with more complex products and services, with a number of branches (or subsidiaries) offering a wide variety of products, or with diversified customers to be served, a more sophisticated risk assessment process is required.

(III) Before a periodical risk assessment is launched, a bank shall establish the clear assessment methods, and explicitly describe its methodology of risk assessment in the risk assessment report.

(IV) The methodology of risk assessment shall include the factors to be assessed, criteria for scoring or rating (including the applied weights and matrixes), other factors, reasons or specific parameters to be adjusted manually.

(V) The mechanism of risk assessment shall be appropriate for the scale, complexity, and nature of business of a bank. All overseas branches (or subsidiaries) shall be included in the scope of these comprehensive risk assessments for money laundering and terrorism financing.

With regard to the branches or subsidiaries of foreign financial institutions in Taiwan, if the risk assessments of their parents are no less than the rules of Taiwan, do not breach the laws and regulations of Taiwan, include these branches and subsidiaries in Taiwan, and the outcomes of such assessments have properly identified the risks of these branches and subsidiaries in Taiwan, these branches and subsidiaries may apply the methodologies and outcomes of their parents.

(VI) The implementation of the risk assessments may be facilitated with the information obtained from both internal and external sources, such as management reports provided by the bank's internal management (e.g. department heads or CRMs), AML/CFT reports released by international anti money laundering organizations or by other countries, or the ML and TF risk information released by the domestic competent authorities (e.g. NRA, SRA reports). Quantified data will facilitate the qualified assess outcomes.

(VII) The frequency of risk assessment is determined by each bank, and there is no mandatory requirement. In the Q&A section of BAROC's Template of Important Notes for Anti-Money Laundering and Combating the Financing of Terrorism to Banks, it is recommended to conduct one comprehensive risk assessment for money laundering and terrorism financing every one or one and half year at least.

(VIII) Except the periodical assessment, if there are any material changes in the internal and/or external environment, (such as major events, significant developments in management and operations, or emerging new threats), a new assessment shall be conducted.

(IX) Banks shall check and review the methodology periodically, to ensure that the risk assessment method takes the impacts resulting from both internal and external changes into consideration.

If the methodology be altered, it is recommended to consider the comparability for the periods spanning over years, and the reasons of the alterations shall be clearly stated.

(X) The implementations and outcomes of the risk assessments shall be properly documented and archived. During the process, the internal executives of the bank shall be kept sufficiently informed through the internal processes.

III. The Process of comprehensive risk Assessments for Money Laundering and Terrorism Financing

In practice, the comprehensive risk assessments for money laundering and terrorism financing include the following main processes:

(I) The design and planning of the risk assessments

(II) The data collections for the risk assessments

(III) The scoring and rating of the risks

(IV) The review of the risk levels

(V) The review of the final risk rating and the approval procedure of the related units.

(VI) The final risk assessment outcomes are provided to the related units or the executives through the internal procedures.

IV. The Assessment Approaches of the comprehensive risk Assessments for Money Laundering and Terrorism Financing

The risk assessment shall identify the inherent risks of the whole bank, assess the control environment, the effectiveness of the risk mitigation measures, and finally assess the residual risks. The following stages may be followed:

(I) Identify the inherent risks of the whole bank: inherent risk refers to the ML and/or TF risks that the bank faces if no control measures are considered.

1. The types, weights, or rating criteria to determine the inherent risks.
   (1) The inherent risk factors shall at least include the clients, areas, products and services, and the channels of transactions or services.
   (2) The basis of the weights or ratings, shall take the different aspects of the risks factors, the risks generated by their characteristics, and the control of the possible impacts into account, or determine such things based on the average or risk-based principles.
2. Definitions of each detailed factors or assessing indicators for each type of the inherent risk factors, and the related information are given in the collected assessment indicators.

   The examples of the indicators and information collections for the inherent risk factors are as follows:
   (1) Client Risk: the indicators to be considered include: type of clients, areas, industries or sectors, and the related information such as numbers of clients for each indicator.
   (2) Area risk: collecting related information such as the number of clients or the transaction volumes of the risk levels for each area.
   (3) Products and Services: the indicators may include: relevance to cash, anonymity, ability to transfer money or value, money received comes from unknown or unrelated third parties. The related information such as numbers of clients or the transaction volume shall be collected.
   (4) The channels of transactions or services: the indicators to be considered include: whether the account is opened not

face-to-face, transactions are executed not face-to-face, involvement of third parties or intermediaries. The related information such as numbers of clients or the transaction volume shall be collected.

3. The abovementioned information shall be collected through the information system by the departments or business lines. All the collected information shall be verified for its accuracy.
4. The scoring or rating for each inherent indicator will be applied to calculate the scores and ratings of each type and the whole bank.
5. The design and implementation of the risk management shall properly include the parts of risk assessment related to the financial institutions in the risk assessment reports released by the competent authorities. For example, the methodologies and outcomes in NRA of ML and TF shall serve as references to design the inherent risk assessment factors or indicators. Taking the “National Risk Assessment of Money Laundering and Terrorism Financing” of Taiwan released in 2018 as an example, the report assesses the vulnerability of each sector and industry to ML and TF with the risk factor types including five indicators: inherent characteristics, nature of the products and services, nature of the business relationships, geographic extent of the business activities, and channels to provide the services.

(II) Assessing the control environment, the effectiveness of the risk mitigation measures (including the efficacies of design and implementation)

1. Control measures refers to the measures, procedures, and actions to prevent the occurrence of ML risks and ensure to

identify the potential risks on time, as well as to the mechanisms and initiatives to ensure the continuous compliance.

2. With regard to general practice, the assessment of the effectiveness of the controlling environment and the risk mitigation measures includes the design of an AML/CFT system, degree of policy compliance, degree and effectiveness of control implementation, degree of automation of operations, and outcomes of internal/external audits and tests.
3. With regard to the basis for the definitions of the control measure types, weights, or ratings, in practices, the major control measures consists of various controlling aspects regarding AML/CFT, such as the anti-money laundering governance, confirmation of clients' identities, verification of names, continuous monitoring of accounts and transactions, report filing for currency transactions exceeding certain thresholds, reporting suspicious ML or TF transactions, continuous staff training, and independent audits, among other things.
4. Identifying the detailed control measures of each type, and defining the levels of the effectiveness for the control measures (i.e. establishing the rating chart): pre-defined scoring criteria, quantifiable ratings (e.g. strong, satisfactory, to be improved, and poor), or in value, to conduct the assessments.

   When assessing the control environment and the risk mitigation measures, the factors to be considered include whether the controls are appropriate, and whether the control measures are effective.

For the scoring criteria for the control measures of each type, the perfect control is deemed achieved when the following conditions are satisfied:

(1) Full compliance and implementation of the related procedures and policies

(2) Automatic control measures are implemented

(3) No material audit or inspection defects found

5. The assessed units are invited to assess the effectiveness of their own control measures according to the degree of implementation and materialization through questionnaires, self-inspection, or information collections.
6. Based on the outcomes of these self-assessments or such information collection, the total scores and ratings of each control measures are calculated. Supporting evidence may be requested from the assessed units, or the information shall be verified if necessary, or the scores or ratings for certain items may be adjusted when necessary.
7. By considering the nature of their own business, banks may incorporate applicable control measures or high risk outcomes identified in the NRA or SRA to their own control operations, policies, or comprehensive risk assessments for money laundering and terrorism financing.

   For instance, the crimes with high ML threats in the NRA outcomes may be incorporated in the control operations of banks, and the effectiveness of the control may be assessed in the risk assessment of the banks.

(1) When implementing the review of clients, based on the risk-based approach, the clients shall be identified if they

are involved with negative information related to crimes with high ML threats via name checking.

(2) With regard to high risk of ML and TF crimes, accounts with abnormal transactions shall be screened out according to the red flags established by the competent authorities.

(3) The continuous education training shall be provided to the staff in charge or anti money laundering and countering terrorism financing, in order to reflect the current laws and regulations, business demands, and the development trends of ML and TF, as well as to raise their awareness of the ML and TF risks related to their operations.

(III) Assessing the Residual Risks

With the outcomes of each assessment, the residual risk level is determined after the controls mitigating the risks. The total rating of these residual risks is determined by the methodologies. The ratings may be low, medium, medium to high, and high risk.

V. After the comprehensive risk assessments for money laundering and terrorism-financing, it is recommended to prepare a rectification plan according to the materialization of the controls and the level of the residual risks, and the following actions shall be taken:

(I) The risk appetite means the types and levels of risks that banks are willing to assume according to their operational strategies and goals.

The residual risks shall be verified as to whether they match with the risk appetite. If not, a risk-reducing rectification plan shall be prepared with the risk-based approach.

(II) Even when the residual risks match with the risk appetite, a rectification plan may be prepared for improvements on non-compliance with the risk mitigation measures, ineffectiveness, or insufficient risk mitigation measures.

(III) The rectification plan may include a policy plan and an implementation plan. Based on their nature, these rectification plans may be considered for integration into the comprehensive anti-money laundering and countering terrorism financing plan.

(IV) Please note that a rectification plan does not affect the outcome of a current risk assessment, but may only affect the next assessment outcomes depending on how they are implemented.

(V) The assessment outcomes shall be communicated to the executives of all departments by the unit in charge through the internal process.

(VI) The head of anti-money laundering and countering terrorism financing shall present the outcomes of the comprehensive risk assessment for money laundering and terrorism financing, the applications of resources, and the priorities of the decided rectifications to the board and the executives.

The board and the executives shall review the status of the risks of money laundering and terrorism financing, the ineffectiveness of the control measures or implementations, and the rectifications plans to be taken, as well as ensure the application of resources, and whether the priorities of the decided rectifications are consistent with the identified risks.

For the branches of foreign banks in Taiwan, the personnel authorized by their head office are responsible for the matters related to the board of directors stated in this text.

(VII) Upon completion or update, a risk assessment report shall be submitted to the Financial Supervisory Commission for future reference.