The Shanghai Commercial & Savings Bank, Ltd.
Group-Level Anti-Money Laundering & Countering the Financing of Terrorism Policy

Drafted by Compliance & Legal Department	2017.08.19
Revised by Compliance Department	2018.06.29
Revised by Compliance Department	2019.03.23
Revised by Compliance Department	2020.06.19
Revised by Compliance Department	2021.03.27
Revised by Compliance Department	2023.03.23
Revised by Compliance Department	2023.08.11

Article 1 Objective

The Shanghai Commercial & Savings Bank, Ltd. (hereinafter referred to as the "Bank") Group-Level Anti-Money Laundering and Countering the Financing of Terrorism policy (hereinafter referred to as " Group-Level AML/CFT Policy") is adopted to provide management framework and guidelines for the practices of all the Bank's business units, including head office, local and foreign branches and subsidiaries as specified in Article 3, to comply with relevant laws and regulations in Anti-Money Laundering and Countering the Financing of Terrorism (hereinafter referred to as "AML/CFT"). The Group-Level AML/CFT Policy implementation and control measures should apply a risk-based approach and take into account the diversity of customer and industry characteristics, and shall be reviewed annually.

Article 2 Definition

The crime of money laundering is committed by any person who[1]：

1. knowingly disguises or conceals the origin of the proceeds of specified unlawful activity, or transfers or converts the proceeds of specified unlawful activity to help others avoid criminal prosecution;
2. disguises or conceals the true nature, source, the movement, the location, the ownership, and the disposition or other rights of the proceeds of specified unlawful activity; or
3. accepts, obtains, possesses or uses the proceeds of specified unlawful activity committed by others.

Terrorist financing is the financing of terrorist acts, terrorists, and terrorist organizations.[2]

[1] 2018.11.7 Article 2,「Money Laundering Control Act」

[2]2018.11.7 Article 1「Counter-Terrorism Financing Act」

Article 3 The Scope of Application and Compliance Guideline

The Group-Level AML/CFT Policy is applicable to the following subjects, and the compliance guidelines are as follows accordingly:

1. For head office and local branches: the implementation of AML/CFT measures shall comply with relevant domestic laws and regulations.
2. For foreign branches: the implementation of AML/CFT measures shall be the same as that of the head office on condition that local regulatory requirements are met. In the case that regulatory requirements of the jurisdictions of a branch are different from those of head office, the branch should comply with the stricter ones. If there are any doubts in determining whether regulatory requirements are stricter or less strict, the Bank should follow the determination of competent authorities where the Bank's head office is located. If a branch is not allowed to implement the measures of head office due to conflicting with foreign regulatory requirements, the Bank should apply appropriate additional measures to manage money laundering and terrorism financing (hereinafter referred to as "ML/TF") risks and inform Financial Supervisory Commission.[3]
3. For the financial institution subsidiaries which shall comply with the AML/CFT laws and regulations according to the laws and regulations of the jurisdictions where it is located (hereinafter referred to as "FIS"): the implementation of AML/CFT measures shall be the same as prescribed in the preceding paragraph[4].
4. For the designated non-financial institution subsidiaries which shall comply with the AML/CFT laws and regulations according to the laws and regulations of the jurisdictions where it is located (hereinafter referred to as "DNFIS"): the DNFIS shall adopt the Group-Level AML/CFT Policy where applicable based on the scale of business and the requirements of the AML/CFT laws and regulations of the the jurisdictions where it is located.

Article 4 Internal control system for AML/CFT[5]

[3] 2021.12.14 Paragraph 5, Article 6「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」

[4] 2018.11.09. Paragraph 5, Article 6「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」

[5] 2019.04.23 Article 2「Template of Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism of Banks」

The internal control system for AML/CFT shall include at least the follows:

1. Establishing relevant written policies and procedures for identifying, assessing and managing the risk of ML/TF.
2. Establishing AML/CFT programs based on the results of the risk assessment.
3. Establishing procedures for supervising the compliance of AML/CFT regulations and the implementation of AML/CFT programs.

Article 5 Anti-Money Laundering and Countering Terrorism Financing program[6]

The AML/CFT program shall include the following rules, procedures and controls, and shall be reviewed periodically:

1. Customer due diligence;
2. Watch list filtering on customers and related parties of a transaction;
3. Ongoing monitoring of accounts and transactions;
4. Correspondent banking business;
5. Record-keeping;
6. Filing currency transaction report (CTR) ;
7. Filing suspicious ML/TF transaction report (STR).
8. Appointment of a compliance officer at the management level in charge of AML/CFT compliance matters;
9. Procedures for screening and hiring employees;
10. An ongoing employee training program;
11. An independent audit function to test the effectiveness of AML/CFT system; and
12. Other matters required by AML/CFT related regulations.

Article 6 Risk-based approach

The Bank (including subjects specified in Article 3) shall, in accordance with relevant rules and regulations, apply a risk-based approach to establish policies and procedures for identifying, assessing and managing ML/TF risks. The risk assessment should consider all risk factors and at least cover the aspect of customers, geographic areas, products and services, transactions or delivery channels, etc. The results of risk assessment shall be used to help the Bank (including subjects specified in Article 3) develop prevention and mitigation measures that are commensurate with the ML/TF risks identified, determine the allocation

[6] 2021.12.14. Paragraph 3, Article 6「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」

of resources on AML/CFT, establish internal control system, and establish and implement policies, procedures and measures that are necessary in AML/CFT programs. ◦

The Bank's Group-level Risk Appetite is '' Moderate''. When the result of the group-level or the Bank's (including subjects specified in Article 3 respectively) enterprise-wide ML/TF risk assessment exceeds the Risk Appetite, the Bank shall establish appropriate Mitigation Measures.

The Bank should establish control measures according to the risks identified, including determining appropriate control measures according to a customer's level of risk. For a high-risk customer, the Bank should obtain the approval of senior management before establishing business relationship.

Article 7 AML/CFT culture

The board of directors and senior management should understand the Bank's ML/TF risks and the operation of AML/CFT programs, and adopt measures to create a culture of AML/CFT compliance.

Article 7-1 Customer Acceptance Principles

The Bank (including subjects specified in Article 3) is strictly prohibited from establishing new banking relationship with the following categories of customer:

1. Designated individuals or entities sanctioned by United Nations Security Council (UNSC) and relevant local authorities of the Bank (specified in Article 3);
2. Individuals or entities associated with terrorism activities;
3. Shell banks or a respondent bank which offers financial services to a shell bank;
4. A respondent bank which provides payable through account services to its customers;
5. Individuals or entities with fictitious names, anonymous accounts, numbered accounts or other means to conceal the identity;
6. Entities that have already issued bearer shares; and
7. Gambling business (including online gambling platforms, except for those approved by local regulatory authority).

The Bank (including subjects specified in Article 3) shall establish controlling measures when establishing banking relationship with Online lending platform, Money Service Business (MSB), Virtual Currency Business (including but not limited to Virtual Currency exchanges / transfer/ brokerage services providers/platforms, Virtual Currency wallet

providers, etc.) and Gambling business(which are approved by local regulatory authority).

Article 8 Group-level information sharing, management and supervision

Given the laws and regulations of the jurisdictions are met, the Bank's all foreign branches, FIS, and DNFIS (hereinafter referred to as "Reporting Units") shall share the following information, and shall pay attention to the safeguard of the information shared[7]:

1. Reporting Units shall report AML/CFT relevant information (including but not limited to suspicious ML/FT transactions, investigation results and improvements) to the Head Office of the Bank.
2. When it is necessary for the Bank's AML/CFT purpose, the Bank can require Reporting Units to provide customer, account and transaction information. This should include information and analysis of unusual transactions or activities. Similarly, Reporting Units should receive such information and analysis from these group-level functions when necessary for AML/CFT purposes.
3. Based on risk-based approach and internal management needs, the Bank can regulate other relevant information to be shared.

The Bank shall establish management regime for AML/CFT programs of all branches and subsidiaries, and supervise the implementation of such AML/CFT programs. For the Bank's foreign branches, the Bank would apply graded management in accordance with the risk-based approach[8].

Article 9 Approval levels

The Group-Level AML/CFT Policy shall be approved by the board of directors of the Bank, and the same approval level should be applied to any amendment thereto.

[7] 2021.12.14. Paragraph 4, Article 6「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」; 2018.7.27 「Financial Holdings Anti-Money Laundering and Countering Terrorism Financing Information Sharing Practice」

[8] 2019.1.17「Self-Regulatory Rule Governing Management Regime for Compliance, Anti-Money Laundering and Countering the Financing of Terrorist Foreign Branch(Subsidiary) for Domestic Member of the Bankers Association of the Republic of China」Article 16

The Shanghai Commercial & Savings Bank, Ltd.

Anti-Money Laundering & Countering the Financing of Terrorism Policy

Prepared by Corporate Banking Department 2014.11.15
Revised by Compliance & Legal Department 2016.03.12
2017.01.14
2017.08.19
Revised by Compliance Department 2018.08.18
2019.03.23
2020.03.21
2021.03.27
2023.03.23
2023.08.11
2024.08.16

Article 1 Objective

The Policy is established with reference to "Money Laundering Control Act", "Terrorism Financing Prevention Act", "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", " Template of Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism of Banks ", the relevant regulation on " Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing" and " Template of Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism of Banks " applied to the Bank's concurrent business promulgated by competent authorities, and the Bank's " Group-Level Anti-Money Laundering& Countering the Financing of Terrorism Policy".

The purpose of the Policy is set for Anti-Money Laundering and Countering the Financing of Terrorism (hereinafter referred to as "AML/CFT"), which includes: the methods to identify and assess money laundering and terrorist financing (ML/TF) risks in business and establish AML/CFT programs, etc., as a basis for implementation. The Policy should be reviewed annually.

Article 2 Risk-based approach

The Bank should, in accordance with relevant rules and regulations, apply a risk-based approach to establish policies and procedures for identifying, assessing and managing ML/TF risks. The risk assessment should consider relevant risk factors that at least cover the aspect of customers, geographic areas, products and services, transactions or delivery channels, etc. The result of the risk assessment should be used to help the Bank to develop prevention and mitigation measures that are commensurate with the ML/TF risks identified, determine the allocation of resources on AML/CFT, build internal control system, and establish and implement policies, procedures and measures that are necessary in AML/CFT programs.

Article 3 Identify, access and manage ML/TF risks[9]

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

The Bank's Risk Appetite is '' Moderate''. When the result of the ML/TF risk assessment exceeds the Risk Appetite, the Bank shall establish appropriate Mitigation Measures.

The periodic enterprise-wide ML/TF risks assessment should be based on following risk factors:

1. The nature, scale, diversity and complexity of businesses.
2. Target markets.
3. Volumes and sizes of transactions: considering the usual transaction activities of the Bank and characteristics of the customers.
4. 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.
5. Businesses and products: including the channels and manners used to provide customers businesses and products, and the way to conduct customer due diligence, such as the extent of using information

[9] 2021.12.14 Article 6, "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''.,2019.04.23 Article 8, "Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program".

system and whether relying on third parties to perform due diligence.

6. The examination results of internal auditors and supervisory authorities.

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

1) Management reports provided by the Bank's management (such as head of business unit, relationship managers, etc.)
2) Relevant AML/CFT reports published by international anti-money laundering organizations and other countries.
3) Information of ML/TF risk released by the Competent Authorities.

The Bank's enterprise-wide ML/TF risk assessment results should be used as a basis to develop AML/CFT programs. The 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, such as a material incident, material development in management and operation, or relevant new threats, the Bank should re-perform the assessment.

After the risk assessment report is completed or updated, it shall be reviewed by the AML&CFT Committee and approved by the board of directors, and then submitted to Financial Supervisory Commission ("FSC")[10].

Article 4 Determine specific risk categories[11]

The Bank should 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 categories should cover at least geographic areas, customers, and products, services, transactions or delivery channels, etc.

The bank should further analyze each risk category to determine detailed risk factors.：

1、Geographic risk:

[10] 2021.02.08 "Template of Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism of Banks and Relevant Regulations Q&A'' Q7.

[11] 2019.04.23 Article 3, "Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program".

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

2、Customer risk:

1) The Bank should take into 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 determining the customer's level of risk, the 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 relationship.
    5. The transaction amount with which the customer first establishes business relationship.
    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.

3、Product and service, transaction or delivery channel risk:

1) The Bank should identify products and services, transactions or delivery channels that have higher ML/TF risk based on the nature of individual product and service, transaction or delivery channel.
2) The Bank should, before launching a new product and service or business (including new payment method, 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 and service, transaction or delivery channel risk factors are as follows:
    1. The extent of associating with cash.
    2. The channel to establish business relationship or process transaction, including whether it allows non-face-to-face transactions, and whether it is a new payment method 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.

Article 5 Customer risk assessment and customer's level of risk

With respect to a new customer to establish business relationship, the Bank should determine the customer's level of risk. With respect to an existing customer, the Bank should re-assess customer risk in accordance with its risk assessment policies and procedures. The Bank should conduct due diligence to existing customers on the basis of materiality and risk, and after taking into account the time and information sufficiency of last due diligence, review the existing business relationships and adjust the level of risk at appropriate times. Such appropriate times should at least include[12]:

1. When the customer opens a new account or establishes a new business relationship.

[12] 2019.04.23 Article 6, “Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program”.

2. Time to conduct periodic review determined on the basis of the customer's materiality and risk.
3. When the Bank knows a material change occurs in the customer's identification and background information.
4. When the Bank reports a suspicious ML/TF transaction or other events that may result in substantial change in customer risk profile occur.

The Bank should review periodically the sufficiency of the information for identifying customers and their beneficial owners, and ensure the timely update of such information, especially for those high-risk customers reviewed at least annually[13].

According to "Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program", the 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, the 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[14]. (**Annotate:** Nevertheless, according to the Bank's ''Directions Governing Anti-Money Laundering & Countering the Financing of Terrorism'', **the Bank SHOULD NOT ESTABLISH BUSINESS RELATIONSHIP WITH** 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.)

Furthermore, the 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.

The Bank's rules to determine the level of customer risk are as follows[15]:

1. According to the specific risk categories adopted, the Bank uses a 3-level classification to profile customer risk, "high-risk", "medium risk", and "low risk".

[13] 2021.12.14 Paragraph 3, Article 5, "Regulations Governing Anti-Money Laundering of Financial Institutions", 2019.04.23 Article 6, "Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program".

[14] 2019.04.23 Article 5, "Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program".

[15] 2019.04.23 Article 4, "Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program".

2. The Bank should not disclose a customer's level of risk to the customer or any person that is unrelated to AML/CFT obligations.

Article 6 Risk-Controlling Measures [16]

The Bank should establish control measures according to the risks identified to mitigate or prevent such money laundering risk. The Bank should determine appropriate control measures according to a customer's level of risk. With respect to such control measures, for a high-risk customer and a customer with a specific high-risk factor, the Bank should take different measures to effectively manage and mitigate identified risks. Following are examples:

1. Conduct enhanced due diligence, for examples:

1) Obtain relevant information about account opening and transaction purpose: such as the purpose of account, expected client transaction activities, etc.
2) Conduct the asset valuation for a client: obtain the client's sources of wealth, sources of fund for transactions, types and quantities of assets to conduct the asset valuation for a client.
3) Obtain an entity client's further business information: understand the client's latest financial situation, commercial activities and business relationship information to establish the source of assets, source of funds and destination of funds.
4) Obtain descriptions and information about transactions going forward or completed.
5) Conduct site visits or telephone surveys based on client patterns to verify the client's actual operating status.

2. Obtain the approval of senior management before first establishing a business relationship or establishing a new business relationship.
3. Increase the frequency of customer due diligence, at least annually.
4. Conduct enhanced ongoing monitoring of the business relationship.

In accordance with FATF recommendations in practices, the Bank may take simplified measures in a lower risk situation. Such simplified measures should be commensurate with the lower-risk factors. Examples of simplified measures that may be applied include:

[16] 2019.04.23 Article 7, "Guidelines to Banks on Money Laundering and Terrorist Financing Risks Assessment and Relevant Prevention Program".

1. Reducing the frequency of updates of customer identification information.
2. Reducing the degree of ongoing monitoring and scrutinizing transactions based on a reasonable monetary threshold.
3. Exempting from collecting specific information or conducting specific measures as to the purpose and nature of business relationships if the Bank may infer this from the type of transactions or business relationships.

Simplified measures, however, should not be permitted in one of the following situations:

1、Customers are from high ML/TF risk jurisdictions, which include but are not limited to the jurisdictions, published by international anti-money laundering organizations and notified by FSC, that have serious deficiencies in AML/CFT, and other jurisdictions that fail to comply with or completely comply with the recommendations of such organizations.

2、The Bank has sufficient reason to suspect the customers or transactions may be involved in ML/TF.

Article 7 AML/CFT program

The Bank should establish AML/CFT program based on ML/TF risks and business scale to manage and mitigate identified risks, such program should also include enhanced control measures for higher risk customers and transactions. The Bank's AML/CFT program should include the procedures and control measures stipulated in Articles 8 to 18 of the Policy herein and should be implemented in accordance with the Bank's Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism[17].

Article 8 Verify the Customer's Identity

The Bank should stipulate policies on the situations, methods, and procedures of verifying the customer's identity. When the customer is a legal person, an organization or a trustee, the Bank should understand the business nature of the customer or trust (including trust-like legal

[17] 2018.11.09 Subparagraph 2 Paragraph 1 Article 6, Paragraph 3Article 6, "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''

arrangements), identify and verify the customer identity[18], identify the beneficial owners of the customer, and determine the entity that is not subject to the requirements of identifying and verifying the identity of beneficial owners.

The Bank is strictly prohibited from establishing new banking relationship with the following categories of customer:

1. Designated individuals or entities sanctioned by United Nations Security Council (UNSC) and relevant local authorities of the Bank;
2. Individuals or entities associated with terrorism activities;
3. Shell banks or a respondent bank which offers financial services to a shell bank;
4. A respondent bank which provides payable through account services to its customers;
5. Individuals or entities with fictitious names, anonymous accounts, numbered accounts or other means to conceal the identity;
6. Entities that have already issued bearer shares;
7. The customer is a legal person with any of the following type of business:
   1)Gambling business (including online gambling platforms, except for those approved by local regulatory authority)
   2)Online lending platform, Money Service Business (MSB), Virtual Currency Business (including but not limited to Virtual Currency exchanges / transfer/ brokerage services providers/platforms, Virtual Currency wallet providers, etc.) However, for this 2), an exception can be allowed to establish new business if the customer has obtained approval from the AML Committee.

Article 9 Watch list filtering on customers and related parties of a transaction[19]

The Bank should establish policies and procedures for watch list filtering on customers and related parties of transactions, by applying a risk-based approach.

The policies and procedures for watch list filtering should include at least matching and filtering logic, the implementation procedures and

[18] 2018.11.14 Paragraph 5, Article 3, "Regulations Governing Anti-Money Laundering of Financial Institutions".
[19] 2018.11.14 Article 8, "Regulations Governing Anti-Money Laundering of Financial Institutions".

evaluation standards, and should be documented. The Bank should record the result of filtering operations, and keep such record.

Article 10 Ongoing monitoring of accounts and transactions[20]

The Bank should use a database to consolidate basic information and transaction information on all customers for inquiries by the head office and branches for AML/CFT purpose to strengthen the Bank's capability of account and transaction monitoring. As to customer information made by various units, the Bank should establish internal control procedures for requests and inquiries, and should exercise care to ensure the confidentiality of the information.

For account and transaction monitoring, the Bank should use a risk-based approach to establish policies and procedures which include at least complete ML/TF monitoring indicators, and carrying out the setting of parameters, threshold amounts, alerts and monitoring operations, the procedures for examining the monitored cases and reporting standards. In addition, based on the business nature of the Bank, the monitoring processes should include the suspicious indicators published by each trade association and the additional ones developed by the Bank in reference to its ML/TF risk assessment or daily transaction information. The established policies and procedures should be documented and the Bank should utilize information system to assist in the detection of suspicious ML/TF transactions.

The Bank should review policies and procedures for account and transaction monitoring based on AML/CFT regulations, nature of customers, business size and complexity, ML/TF trends and related information gathered from internal and external sources, and its risk assessment results, and update those policies and procedures periodically.

The Bank should document its ongoing account and transaction monitoring operation and maintain the records.

Article 11 Correspondent banking[21]

The Bank should comply with the following provisions with respect to establish correspondent banking and other similar relationships:

---

[20] 2018.11.14 Article 9, "Regulations Governing Anti-Money Laundering of Financial Institutions".

[21] 2021.12.14 Article 3, "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''.

1. Gather sufficient publicly available information to fully understand the nature of the respondent bank's business and to determine its reputation and quality of management, including whether it has complied with the AML/CFT regulations and whether it has been investigated or received administrative sanction in connection with money laundering or terrorist financing (ML/TF);
2. Assess whether the respondent bank has adequate and effective AML/CFT controls;
3. Before establishing relationships with a respondent bank, the approval from the President is required if the respondent bank is assessed as low/medium risk, and the approval from the Bank's AML&CFT Committee is required if the respondent bank is assessed as high risk;
4. Document the respective AML/CFT responsibilities of each party;
5. It is prohibited for the Bank to establish correspondent relationship with other banks involving the maintenance of 「payable–through accounts」;
6. The Bank is prohibited from establishing correspondent relationship with any shell banks or any foreign financial organizations permitting any shell banks to use their accounts;
7. For a respondent bank that is unable to provide the aforementioned information upon the request of the Bank, the Bank may decline the respondent bank's application to open an account, suspend transactions with the respondent bank, file a suspicious ML/TF transaction report or terminate business relationship with it; and
8. The aforementioned provisions applied when the respondent bank is a foreign branch (subsidiary) of the Bank.

Article 11-1 Assisting foreign institution in engaging in activities associated with electronic payment business

The Bank cooperates with or assists foreign institution in engaging in activities associated with electronic payment business within the territory of R.O.C should have relevant procedures in place, including at least the following[22]:

[22] 2021.06.15 Article 11, ''Template of Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism of Electronic payment institution''.

1. Collect enough publicly available information to fully understand the nature of the business of the foreign institution, and evaluate its goodwill and management quality, including whether it complies with the laws and regulations of AML&CFT.
2. Evaluate that the foreign institution has considerable control policies and execution for AML&CFT.
3. Obtain approval from the President before cooperating with or assisting foreign institution in engaging in activities associated with electronic payment business within the territory of R.O.C.
4. Documents to prove respective responsibilities for AML&CFT.

Article 12 Record-keeping[23]

The Bank should keep records on all business relationships and transactions with customers in hard copy or electronic form in accordance with following provisions:

1. The Bank should maintain all necessary records on transactions, both domestic and international for at least five years or a longer period as otherwise required by law.
2. The Bank should keep all the following information for at least five years or a longer period as otherwise required by law after the business relationship is ended, or after the date of the occasional transaction:
    1) All records obtained through the CDD measures, such as copies or records of official identification documents like passports, identity cards, driving licenses or similar documents.
    2) Account files (including e-payment accounts and the accounts of credit card holders) or contract files.
    3) Business correspondence information, including inquiries to establish the background and purpose of complex, unusual large transactions and the results of any analysis undertaken.
3. Transaction records maintained must be sufficient to the reconstruction individual transactions if necessary, to provide evidence for prosecution of criminal activity.
4. The Bank should ensure that transaction records and CDD information will be available swiftly to the competent authorities when requested with appropriate authority.

[23] 2021.12.14 Article 12, "Regulations Governing Anti-Money Laundering of Financial Institutions"

Besides, the Bank should maintain the records on the results of filtering operations, ongoing account and transaction monitoring operation, the data reported to the Investigation Bureau, Ministry of Justice ("Investigation Bureau" hereunder) on any cash transactions above a certain amount, and relevant documents of suspicious transaction report on money laundering or terrorist financing, in accordance with Paragraph 1 of Article 12 herein.

Article 13 Report on cash transactions above a certain amount [24]

The Bank should comply with the following provisions with respect to cash transactions above a certain amount:

1. Verify the identity of the customer and keep relevant transaction records
2. Conduct CDD measures in accordance with the Bank's relevant provisions on reporting procedures.
3. Except specifically stipulated otherwise in relevant regulations, the Bank should report the transaction to the Investigation Bureau in a format prescribed by the Investigation Bureau via electronic media in five (5) business days after the completion of transaction. If the Bank is unable to file a report via electronic media with a legitimate reason, the Bank may file a written report after obtaining the consent of the Investigation Bureau.

Article 14 Suspicious transaction report on money laundering or terrorist financing[25]

The Bank should file suspicious ML/TF transaction reports in accordance with following provisions:

1. For transactions related to account, the monitoring patterns, or other situations that are deemed as suspicious ML/TF activities, the Bank should complete the review process as quickly as possible to determine whether the transaction is suspected of involving ML/TF activity, and shall retain records.
2. Where review has resulted in a determination that a transaction is suspected of involving ML or TF activity, regardless of the amount of the transaction, the Bank should promptly file a STR with the Investigation Bureau in a format prescribed by the Bureau after the

[24] 2021.12.14Article 13, "Regulations Governing Anti-Money Laundering of Financial Institutions"
[25] 2021.12.14Article 15, "Regulations Governing Anti-Money Laundering of Financial Institutions"

report has been approved by the responsible chief compliance officer. The report shall be filed within two business days of said approval. The same shall apply to attempted (uncompleted) transactions.

3. For obviously significant suspicious ML/TF transactions of urgent nature, the Bank should file a report as soon as possible to the Investigation Bureau by fax or other available means and follow it up with a written report.

Article 15 Chief AML/CFT compliance officer and Dedicated compliance unit:[26]

The Bank should be staffed with adequate number of AML/CFT personnel and resources appropriate to the size and risks, and etc. The board of directors appoints the Executive Vice President of Compliance Department to act as chief AML/CFT compliance officer, vests the officer full authority in coordinating and supervising AML/CFT implementation, and ensures such personals and chief AML/CFT compliance officer do not hold concurrent posts that may have a conflict of interest with their AML/CFT responsibilities. In addition, the Bank sets up an independent AML/CFT dedicated compliance unit under the Compliance Department. Such unit may not handle business other than AML/CFT.

Dedicated compliance unit or chief compliance officer aforementioned are in charge of following duties:

1. Supervising the planning and implementation of policies and procedures for identifying, assessing and monitoring ML/TF risks.
2. Coordinating and supervising the implementation of the Bank-wide ML/TF risk identification and assessment.
3. Monitoring risks related to ML/TF.
4. Developing AML/CFT programs.
5. Coordinating and supervising the implementation of AML/CFT programs.
6. Confirming the compliance with relevant AML/CFT regulatory requirements, including relevant specimen or self-regulatory rules formulated by the financial services trade association and accepted by Financial Supervisory Commission for recordation.

[26] 2021.12.14Article 7, "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''.

7. Supervising the reporting of suspicious ML/TF transactions, the properties or property interests and the locations of properties or property interests of individuals or legal entities designated by the "Terrorism Financing Prevention Act" to the Investigation Bureau.

For the Bank's domestic branches and business units, the Operation & Compliance Manager / Senior Compliance Manager is appointed to act as the AML/CFT supervisory officer. For the Bank's foreign branches, Chief Executive is appointed to act as the supervisory officer. Supervisory officer should take charge of supervising AML/CFT related matters of the belonged branch/business unit and conduct self-inspection.

For the Bank's foreign branches, the Senior Compliance Manager is appointed to act as the AML/CFT compliance Manager and should take charge of the coordination and supervision of AML/CFT related matters[27]. The appointment should comply with the local regulations and the requirements of the local authorities of the foreign branches' jurisdiction. The AML/CFT compliance Manager is vested with full authority in the coordination and supervision of AML/CFT related matters, including reporting directly to the chief AML/CFT compliance officer of the head office[28]。

Article 16 Procedures for hiring employees

The Bank should establish high standards procedures for employee screening and hiring, including examining whether the prospective employee has character integrity and the professional knowledge required to perform its duty [29].

The Bank's chief AML/CFT compliance officer, the personnel of dedicated AML/CFT unit, and the domestic branches supervisory officers should meet competent authorities' qualification requirements before/after the appointment.

---

[27] 2021.12.14 Paragraph 4,Article 7, "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''..

[28] 2021.12.14Paragraph 5,Article 7, "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''.

[29] 2021.12.14Paragraph 1,Article 9, "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 Bank's foreign branches supervisory officer and AML/CFT Compliance Manager and personals should have AML expertise, and should be familiar with local regulations.

Article 17 On-the-job training program

The Bank should arrange AML/CFT training programs that meet the rules set by the competent authorities.

The Bank's directors, independent directors, president, chief AML/CFT compliance officer, the personnel of dedicated AML/CFT unit, compliance officers, internal auditors and relationship managers, every foreign and domestic branch's Senior Compliance Managers, supervisors, and AML/CFT personnel, new employees and other staff, should take AML/CFT training programs, complying the rules set by the competent authorities, according to the nature of their job characteristics[30]

Article 18 Internal Audit System

The Bank should establish independent internal audit system to assess whether AML/CFT program is implemented effectively. The relevant regulations of their operational procedures should be included in the self-inspection and internal audit items, and enhanced if necessary[31].

The Bank's Auditing Department should, in compliance with relevant regulations, audit the following matters and submit audit opinions[32]:

1. Whether the ML/TF risk assessment and the AML/CFT program meet the regulatory requirements and are vigorously implemented.
2. The effectiveness of the AML/CFT program.

Article 19 AML/CFT culture[33]

The Bank's Board of Directors holds the ultimate responsibility of ensuring the establishment and maintenance of appropriate and effective AML/CFT

[30] 2021.12.14 Paragraph 3,4,5,Article 9, "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''.

[31] 2021.12.14 Subparagraph 3, Paragraph 1,Article 6, "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''..

[32] 2021.12.14 Paragraph 2, Article 8, "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''.

[33] 2021.12.14 Paragraph 6, Article 6, "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''.

internal controls. The board of directors and senior management of the Bank should understand the Bank's ML/TF risks and the operation of AML/CFT programs, and adopt measures to create a culture of AML/CFT compliance.

Article 20 Group-level information sharing and supervision [34]

Given the laws and regulations of the jurisdictions are met, the Bank's all foreign branches and subsidiaries[35] (hereinafter referred to as "Reporting Units") shall share the following information, and shall pay attention to the safeguard of the information shared[36]:

1. Reporting Units shall report AML/CFT relevant information (including but not limited to suspicious ML/FT transactions, investigation results and improvements) to the Head Office of the Bank.
2. When it is necessary for the Bank's AML/CFT purpose, the Bank can require Reporting Units to provide customer, account and transaction information. This should include information and analysis of unusual transactions or activities. Similarly, Reporting Units should receive such information and analysis from these group-level functions when necessary for AML/CFT purposes.
3. Based on risk-based approach and internal management needs, the Bank can regulate other relevant information to be shared.

I

The AML&CFT Center of the head office shall report the content and effect of the implementation of group-level information sharing to the AML&CFT Committee at least every six months. If there is customer due diligence information sharing between Reporting Units (including beneficial owner), the implementation status should be reported to the Board of Directors at least every six months[37].

The Bank shall establish management regime for AML/CFT programs of all branches and subsidiaries, and supervise the implementation of such

[34] Article 8, "The Shanghai Commercial & Savings Bank, Ltd. Group-Level Anti-Money Laundering & Countering the Financing of Terrorism Policy" ◦

[35] I.e. the subsidiary that shall comply with the AML/CFT laws and regulations according to the laws and regulations of the jurisdictions where it is located.

[36] 2021.12.14 Paragraph 4, Article 6, "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''; 2018.7.27 ''Financial Holdings Anti-Money Laundering and Countering Terrorism Financing Information Sharing Practice''.

[37] 2018.7.27 Paragraph 5, Article 5,''Financial Holdings Anti-Money Laundering and Countering Terrorism Financing Information Sharing Practice''.

AML/CFT programs. For the Bank's foreign branches, the Bank would apply graded management in accordance with the risk-based approach[38].

Article 21 Supplementary provisions

For matters not specified in the Policy herein, the applicable regulations or the Bank's rules should be applied. In the case that regulatory requirements of the jurisdictions where head office and a branch are located are different, the branch should follow the criteria which are higher. However, in case there is any doubt regarding the determination of higher or lower criteria, the Bank should follow the decision of the Financial Supervisory Commission.

If the Bank’s foreign branch is unable to adopt the same criteria as that of the head office due to prohibition from foreign laws and regulations, the Bank should apply appropriate additional measures to manage ML/TF risks, and the AML/CFT Compliance Manager of Bank's foreign branch should report to the AML&CFT Center of the head office, and the AML&CFT Center of the head office should make a report to Financial Supervisory Commission[39]。

Article 22 Approval levels

The Policy should be implemented after the approval of the Board of Directors, and the same approval levels should be applied to any amendment thereto.

[38] 2019.1.17「Self-Regulatory Rule Governing Management Regime for Compliance, Anti-Money Laundering and Countering the Financing of Terrorist Foreign Branch(Subsidiary) for Domestic Member of the Bankers Association of the Republic of China」Article 16.

[39] 2021.12.14 Paragraph 5,Article 6, "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’’.