AML/CFT & CFP Compliance Examination Manual

for Banking Sector

Revised June 2022

Examination Item
A.Risk Assessment
B.Customer Due Diligence
C.Ongoing Monitoring and Filing of Suspicious Transaction Reports
D.Policies andProcedures
E.Organization and Personnel
F.Countering Financing Terrorism
G.Countering Financing Proliferation

AML/CFT & CFP Compliance Examination Manual for Banking Sector

Table of Contents

I. Preface

This manual is designed for financial examiners' reference while assessing the effectiveness of AML/CFT measures conducted by the banking industry (including postal institutions conducting the postal savings and remittances business).

To benefit understanding, the definition of Money Laundering and Terrorist Financing are illustrated as the following.

(A)Money Laundering

(a) Placement.

The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements. Examples may include: dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account, or purchasing a series of monetary instruments (e.g., cashier's checks) that are then collected and deposited into accounts at another location or financial institution. This stage is what the 1st subparagraph of article 2 of Money Laundering Control Act refers to "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."

(b) Layering.

The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper

trail. Examples of layering include wiring or transferring funds to and through numerous accounts in one or more financial institutions. This stage is what the 2nd subparagraph of article 2 of Money Laundering Control Act refers to “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.”

(c) Integration.

Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets. This stage is what the 3rd subparagraph of article 2 of Money Laundering Control Act refers to “accepts, obtains, possesses or uses the proceeds of specified unlawful activity committed by others.”

(B)Terrorist Financing

An effective financial infrastructure is critical to terrorist operations. Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing.

(C)Proliferation Financing

Proliferation financing refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment,

brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

II. Risk-based Approach AML/CFT & CFP Examination

The frequency and depth of examinations on the banking industry conducted by the FSC are based on the results of the inherent ML/TF & PF risks and the effectiveness of control measures adopted by all banks. While conducting examination, the FSC would focus on the control measures the banks adopted for the customers from the sectors that have been identified by National Risk Assessment as presenting higher ML/TF risks, and the products, services, transactions and delivery channels that are more susceptible to the higher risk.

The regulations cited in this manual are only the minimum standards for the banking industry in AML/CFT & CFP regime. Examiners should evaluate the adequacy and effectiveness of AML/CFT & CFP controls based on the bank's own business characteristics and its risk profile. If much failures or weaknesses are uncovered from specific examination item, the examiner should expand testing samples. And If the examined bank identified other products or services and etc. that are not listed in this manual and bear higher ML/FT & PF risks, the examiner should also evaluate the adequacy and effectiveness of AML/CFT & CFP controls of those products or services and etc.

III. Examination Items

No.	Examination Item	Legal Basis
A	**Risk assessment**	
(A)	Whether the bank sets specific risk assessment items based on the identified risks. Specific risk assessment items should cover at least customers, geographic locations, products and services, transactions or delivery channels.	2nd paragraph of Article 6「The ML/TF risk identification, assessment and management mentioned in Subparagraph 1 of the preceding paragraph shall cover at least customers, geographic areas, products and services, transactions or delivery channels」 Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
1	Refer to Appendix A with regard to a risk assessment methodology. However the examiner should heed that the bank may adopt a different approach based on the size, complexity and nature of its business or choose different factors in its risk assessment operation while using the same approach illustrated in Appendix A.	
2	Whether the bank describes in relevant documents the risk assessment approaches, risk assessment items, and detailed risk factors taken into account and the clear definitions of risk assessment items and detailed risk factors, types of control measures (in particular whether there are enhanced controls	1.1st paragraph of Article 6「The AML/CFT internal control system established by a banking business and other financial institutions designated by the FSC and any subsequent amendment thereto shall be approved by its board of directors (council), and shall contain the following:

No.	Examination Item	Legal Basis
	for high-risk products, services, delivery channels, customers or geographic locations identified), customer risk levels and classification rules, overall risk tolerance, and improvement mechanism when risk tolerance is exceeded, and those documents are approved by the bank's board of directors.	1. The policies and procedures to identify, assess and manage its ML/TF risks; 2. An AML/CFT program established based on ML/TF risks and business size to manage and mitigate identified risks, which also includes enhanced control measures for higher risk situations.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission 2. 1st & 2nd subparagraphs of Point 4 「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.」, Guidelines for Banks Regarding Assessment of Money Laundering and Terrorism Financing Risks and Adoption of Prevention Programs(June 28, 2017 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association
3	Whether risk assessment items cover completely the aspects of geographic	

No.	Examination Item	Legal Basis
	locations, customers, products and services, transactions or delivery channels (referred to as “inherent risks” below).	
4	Check whether the bank has appropriately reflected relevant internal and external information into assessments of its own ML/TF (including proliferation financing) risk, and has retained related information. Related information includes, not limited to, the following: communications with the related business units; the results of the national risk assessment (e.g. very high threats, higher-risk lines of business, sector vulnerabilities, and high-risk jurisdictions); sanctioned jurisdictions or sanction lists released by international organizations or foreign governments; money laundering (including proliferation financing) typologies (e. g. "use of the bank's safety deposit boxes a channel for money laundering and/or movement of funds" is included among the money laundering typologies released by the MOJ Investigation Bureau regarding high-risk threats of corruption and bribery).	
5	When the bank develops detailed risk factors for inherent risks, whether the bank fails to consider signs of ML/TF vulnerabilities. For detailed risk factors, the examiner can refer to the 2017.06.28 “Guidelines	

No.	Examination Item	Legal Basis
	Governing Money Laundering and Terrorist Financing Risk Assessment and Relevant Prevention Program Development by the Banking Sector." However the bank may adopt part of the risk factors illustrated in the Guidelines or develop more refined detailed risk factors based on the nature, size or complexity of its business.	
6	Whether the bank assesses ML/TF risks before launching new products or services or new business practices (including new delivery mechanisms, use of new technologies for pre-existing or new products or business practices) and establish documented risk management measures based on the risk assessment result.	Article 4「A banking business and other financial institutions designated by the FSC shall assess ML/TF risks before launching new products, new services or new business practices and establish appropriate risk management measures to mitigate identified risks.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
7	Are customer risk factors applied uniformly throughout the bank? Are there situations where different departments or product lines use different risk factors in customer risk assessment?	
(B)	Has the bank established risk management measures commensurate with its risk profile to mitigate identified risks? For inherent	

No.	Examination Item	Legal Basis
	risks assessed to be higher risks, has the bank adopted clear risk mitigation measures and documented them? (For information on enhanced measures for high-risk items, please refer to: "B. Customer due diligence"; "C. Ongoing monitoring and filing of STRs"; "D. Policies and procedures"; "E. Organization and personnel"; and "G. Countering Financing Proliferation")	
(C)	Production of risk assessment report	
1	Whether the bank generates a risk assessment report and submits the report to the FSC for reference.	1.2nd paragraph of Article 6「The ML/TF risk identification, assessment and management mentioned in Subparagraph 1 of the preceding paragraph shall cover at least customers, geographic areas, products and services, transactions or delivery channels, and contain the following: 1. A risk assessment report shall be documented; 2. The risk assessment shall consider all risk factors to determine the level of overall risk, and appropriate measures to mitigate the risks; 3. There shall be a risk assessment update mechanism in place to ensure that risk data are kept up-to-date; and 4. When the risk assessment is completed or updated, the report shall be submitted to the FSC for recordation.」, Regulations Governing Internal Audit and

No.	Examination Item	Legal Basis
		Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission 2.Poin 3 & 8 of Guidelines for Banks Regarding Assessment of Money Laundering and Terrorism Financing Risks and Adoption of Prevention Programs(June 28, 2017 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association
2	The timing for the bank to update its risk assessment report may include but is not limited to: when introducing a new product or service or changing existing product or service, a certain large number of high-risk customers open or close accounts or the bank undergoes merger and acquisition (that is, when there is significant change in the aspect of customer, geographic location, product and service, transaction or delivery channel covered in risk assessment); the bank should describe specifically the appropriate time to update risk assessment in its internal policy or rules and operating procedures.	
3	The bank's internal policy or rules and operating procedures should describe specifically the frequency of	

No.	Examination Item	Legal Basis
	risk assessment, e.g. once every year and a half, every year, or six months.	
4	Is there any deficiency in the way the bank conducts risk assessment? For example, is full consideration given to qualitative and quantitative factors; is the same risk level assigned to businesses or products with higher inherent risk (correspondent banking, cross border remittance, etc.) and businesses or products with lower inherent risk?	
5	Refer to Appendix A with regard to a risk assessment methodology. However the examiner should heed that the bank may adopt a different approach based on the size, complexity and nature of its business or choose different factors in its risk assessment operation while using the same approach illustrated in Appendix A.	
6	Is there any incongruity in the overall risk assessment result? For example, the overall inherent risk is assessed as “high risk” and its control effectiveness is assessed as “weak”, but the overall risk assessment result is “medium risk.”	
7	Is every risk factor scored and are inherent risk factors and control effectiveness factors scored and combined. For example, customers posing inherent risks include all types of customers (PEP, offshore company, etc.), then there should be scoring criteria for respective type of	

No.	Examination Item	Legal Basis
	customers in terms of inherent risk and control effectiveness. If there are no quantitative criteria and the bank is not able to carry out detailed review, then propose an appropriate improvement plan.	
8	Are all control effectiveness factors considered actually included in the internal control procedures; the examiner should make sampling check inherent risk factors rated as high risk (customers, products and services, service areas, etc.) to determine whether the bank has designed internal controls for mitigating relevant risks which can be matched against the control effectiveness factors considered. If such matching cannot be done, has the bank overestimated the effectiveness of control factors?	
B	**Customer due diligence (CDD)**	
(A)	Measures for verifying customer identity	
1	Examine whether the bank's internal rules and operating procedures include: ① Not accepting or maintaining business relationship with anonymous accounts or accounts in fictitious names. ② Setting the time for conducting CDD. ③ Obtaining information for CDD (including information on customer, any person purporting to act on behalf of the customer,	1. 1st and 2nd paragraphs of Article 7「Financial institutions and designated nonfinancial businesses or professions shall apply a risk-based approach to undertake customer due diligence measures for verifying the identity of the customer and beneficial owner, and keep all information obtained through the customer due diligence measures. The information obtained through the customer due diligence

No.	Examination Item	Legal Basis
	beneficial owner or senior management) and adopting risk-based approach to identity verification (including verification methods and procedure for handling the situation when CDD cannot be completed in time). ④ Retaining relevant data on identifying and verifying customer identity (including data that are apparently conflicting with each other found in the CDD process). ⑤Carrying out name screening on existing customers (including the customer, any person purporting to act on behalf of the customer, beneficial owner or senior management) who apply for a new account. ⑥When the bank relies on a third party to perform CDD, does the bank audit and monitor the third party's use, processing and control of customer information? ⑦ Internal rules and operating procedures for immediately filing suspicious ML/TF transaction report at the time a customer opens an account when necessary. ⑧Conducting CDD measures again when the bank has doubts about the veracity or adequacy of customer data, there is a suspicion of money laundering or terrorist financing in relation to that customer, or there is a material change in the way that the	measures prescribed in the preceding paragraph shall be maintained for at least five years after the business relationship is ended, or after the date of the occasional transaction, unless a longer record-keeping term is required by other laws.」,Money laundering Act(November 7, 2018 Amended), Ministry of Justice 2. 1st and 2nd subparagraphs of Article 3「A financial institution shall comply with the following provisions in undertaking customer due diligence (CDD) measures:1. A financial institution shall not accept anonymous accounts or accounts in fictitious names for establishing or maintaining business relationship.2. A financial institution shall undertake CDD measures when:(1) establishing business relations with any customer;(2) carrying out occasional transactions with respect to: A. a single transaction (including domestic remittances) or a certain number (or greater) of electronic stored value card transactions that meet or exceed a certain amount, or multiple clearly related transactions that in sum total meet or exceed a certain amount; orB. a cross-border wire transfer involving NTD 30,000 or

No.	Examination Item	Legal Basis
	customer's account is operated, which is not consistent with the customer's business profile.	more (including the foreign currency equivalent thereof);(3) there is a suspicion of money laundering or terrorist financing; or(4) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.」, Regulations Governing Anti-Money Laundering of Financial Institutions (November 14, 2018 Amended) , Financial Supervisory Commission 3. 4th and 5th subparagraphs of Article 3「4. The CDD measures to be taken by a financial institution shall be as follows: (1) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information. In addition, a financial institution shall retain copies of the customer's identity documents or record the relevant information thereon. (2) Verifying that any person purporting to act on behalf of the customer is so authorized, identifying and verifying the identity of that person using reliable, independent source documents, data or information. In addition, the financial institution shall retain copies of the person's identity documents or record the relevant information thereon. (3) Identifying the identity of the

No.	Examination Item	Legal Basis
		beneficial owner of a customer and taking reasonable measures to verify the identity of the beneficial owner, including using the relevant data or information from a reliable source. (4) Understanding and, in view of the situation, obtaining relevant information on the purpose and intended nature of the business relationship when undertaking CDD measures. 5. When the customer is a legal person, an organization or a trustee, a financial institution shall, in accordance with the preceding subparagraph, understand the business nature of the customer or trust (including a legal arrangement similar to a trust) and obtain at least the following information to identify the customer or the trust and verify its identity: (1) Name, legal form and proof of existence of the customer or trust.(2) The charter or similar power documents that regulate and bind the legal person or trust, except for any of the following circumstances: A. Customers/entities provided under Item (3) of Subparagraph 7 hereof and insurance products provided under Item (4) of Subparagraph 7 hereof without the situations specified in the proviso of Subparagraph 3,

No.	Examination Item	Legal Basis
		Paragraph 1 of Article 6 herein. B. Engaging in electronic stored value card registration business. C. The customer who is an organization is verified that it does not have a charter or similar power document. (3) Names of relevant persons having a senior management position in the customer. (4) The address of the registered office of the customer, and if different, the address of its principal place of business.」, Regulations Governing Anti-Money Laundering of Financial Institutions (November 14, 2018 Amended), Financial Supervisory Commission 4. 8th to 13th subparagraphs of Article 3「8. An insurance enterprise shall adopt the following measures when the beneficiary(ies) of a life insurance policy, investment related insurance policy or annuity insurance policy have been identified or designated: (1) Obtaining the name and identification document number or registration (incorporation) date of the designated beneficiary; and (2) For beneficiary(ies) that are designated by contract characteristics or by other means, obtaining sufficient information concerning the beneficiary to

No.	Examination Item	Legal Basis
		satisfy the insurance enterprise that it will be able to establish the identity of the beneficiary at the time of the payout. (3) Verifying the identity of the beneficiary(ies) at the time of the payout. 9. A financial institution shall not establish business relationship or conduct occasional transactions with a customer before completing the CDD measures. However, a financial institution may first obtain information on the identity of the customer and its beneficial owner(s) and complete verification after the establishment of business relationship, provided that:(1) The ML/TF risks are effectively managed, including adopting risk management procedures with respect to the conditions under which a customer may utilize the business relationship to complete a transaction prior to verification; (2) This is essential not to interrupt the normal conduct of business with the customer; and (3) Verification of the identities of the customer and its beneficial owner(s) will be completed as soon as reasonably practicable after the establishment of business relationship. A financial institution shall advise its customer in advance that the

No.	Examination Item	Legal Basis
		business relationship will be terminated if verification cannot be completed as soon as reasonably practicable. 10. Where a financial institution is unable to complete the required CDD process on a customer, it should consider filing a suspicious transaction report on money laundering or terrorist financing (STR) in relation to the customer. 11. If a financial institution forms a suspicion of money laundering or terrorist financing and reasonably believes that performing the CDD process will tip-off the customer, it is permitted not to pursue that process and file an STR instead. 12. The CDD process for e-payment accounts shall follow relevant provisions in the Regulations Governing Identity Verification Mechanism and Transaction Limits for Users of Electronic Payment Processing Institutions, to which the provisions of Subparagraphs (4) ~ (7) hereof do not apply. 13. The provisions of Item (3) of Subparagraph 4 and Subparagraph 6 hereof do not apply to electronic stored value card registration operation. 」, Regulations Governing Anti-Money Laundering of Financial Institutions (November

No.	Examination Item	Legal Basis
		14, 2018 Amended) , Financial Supervisory Commission 5. Bank Accepting Customer Opening Digital Deposit Account Online Guideline 6.Article 7「 A financial institution should perform CDD measures. However, if it is otherwise permitted by laws or regulations of the FSC that a financial institution may reply on third parties to perform the identification and verification of the identities of customers, agents and beneficial owners or the purpose and intended nature of the business relationship, the financial institution relying on the third party shall still bear the ultimate responsibility for CDD measures and comply with the following provisions: 1. A financial institution relying on a third party should be able to immediately obtain the necessary CDD information. 2. A financial institution should take adequate steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay. 3. A financial institution shall make sure that the third party it relies on is regulated, supervised

No.	Examination Item	Legal Basis
		or monitored, and has appropriate measures in place for compliance with CDD and record-keeping requirements. 4. A financial institution shall make sure that the jurisdiction where the third party it relies on is based has AML/CFT regulations in place consistent with the standards set out by the FATF.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission 7.Article 16「An electronic payment institution is deemed to have carried out the required identity verification process for a user, provided that the outsourced service provider has performed the identity verification of the users by following a procedure not less than the requirements set out in Articles 9 ~ 11 and Articles 13 ~ 15 hereof. If an electronic payment institution engage an outsourced service provider to perform the identity verification process, the regulations set forth in Article 7 of the Regulations Governing Anti-Money Laundering of Financial Institutions shall apply to the institution.」, Regulations Governing Identity Verification Mechanism and Transaction Amount Limits of Electronic

No.	Examination Item	Legal Basis
		Payment Institutions (June 30, 2021 Amended), Financial Supervisory Commission 8.4th subparagraph of Article 5「A financial institution can rely on existing customer records to undertake identification and verification without the need to repeatedly identify and verify the identity of an existing customer when carrying out transactions. However, a financial institution shall conduct CDD measures again in accordance with Article 3 when it has doubts about the veracity or adequacy of the records, where there is a suspicion of ML/TF in relation to that customer, or where there is a material change in the way that the customer's transaction is conducted or the customer's account is operated, which is not consistent with the customer's business profile.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended), Financial Supervisory Commission
2	Does the CDD process established by the bank cover all accounts (e.g. safe deposit box, trust, digital deposit, credit card product, etc.) or services (e.g. occasional transactions handled for a customer without a bank account) provided by the bank?	
3	Whether the bank includes its CDD	

No.	Examination Item	Legal Basis
	operation in its internal audit system and employee training program.	
4	Check whether the bank updates the following in a timely manner: (i) its sanctions list; (ii) the list of terrorists and terrorist organizations adopted by the bank in accordance with its policies; and (iii) its list of countries or regions with high risk of money laundering or terrorist financing or proliferation financing (including, not limited to, the jurisdictions, published by international anti-money laundering organizations and notified by FSC, that have serious AML/CFT deficiencies, and other jurisdictions recommended by international anti-money laundering organizations). Check whether the bank uses these lists to screen the names of new customers.	Article 8「Financial institutions shall comply with the following provisions in their watch list filtering programs on customers and connected parties of transactions : 1. A financial institution shall establish policies and procedures for watch list filtering, based on a risk-based approach, to detect, match and filter whether customers, or the senior managerial officers, beneficial owners or connected parties of the customers are individuals, legal persons or organizations sanctioned under the Terrorism Financing Prevention Act or terrorists or terrorist groups identified or investigated by a foreign government or an international organization. 2. The policies and procedures for watch list filtering shall include at least matching and filtering logics, implementation procedures and evaluation standards, and shall be documented. 3. A financial institution shall document its name and account filtering operations and maintain the records for a time period in accordance with Article 12.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission

No.	Examination Item	Legal Basis
5	When necessary, the examiner can conduct verification according to the following procedure: ①Select, based on the bank's risk assessment result, internal audit report and prior examination reports, a sample of new accounts for various businesses (e.g. deposits, trust, loan, credit card product, online banking, etc.) opened since the end of previous examination (including higher risk accounts, accounts approved without completing CDD process, new accounts opened by existing higher risk customers, accounts opened with exceptions, and accounts for which CDD is conducted by a third party), accounts are suspicious of money laundering or terrorist financing, and accounts where the transactions or how the account is operated is not consistent with the customer's business profile. ② Use the aforementioned samples to examine whether the bank performs CDD on customers (including customer, its agent, beneficial owner or senior management), and obtain and keep relevant customer data in accordance with relevant regulations and internal rules and operating procedures, and conduct sanction screening on customers (including customer, beneficial	

No.	Examination Item	Legal Basis
	owner or senior management). ③ Evaluate whether the bank's criteria for allowing accounts opened with exceptions affect the effectiveness of its CDD. ④ Screen occasional transactions carried out by customers without a bank account (cash transactions above a certain amount or electronic stored value cards above a certain quantity or multiple apparently related cash transactions that is above a certain amount when combined, cross-border wire transfers involving NTD 30,000 or more (including the foreign currency equivalent thereof) to examine whether the bank has undertaken CDD on customers. ⑤Examine whether the bank keep customer identity information in accordance with its internal rules and operating procedures and keep the information for at least 5 years after the business relationship is ended, or after the date of the occasional transaction. ⑥ Examine whether the bank performs CDD again when there is a suspicion of money laundering or terrorist financing in relation to that customer, or when there is a material change in customer's transactions or in the way that the customer's account is operated, which is not consistent with the	

No.	Examination Item	Legal Basis
	customer's business profile. However when the bank forms a suspicion of money laundering or terrorist financing and reasonably believes that performing the CDD process will tip-off the customer and chooses not to pursue that process, determine whether the bank files a suspicious transaction report.	
(B)	CDD and identification of customer's beneficial owner	1.6th subparagraph to 9th subparagraph of Article 3「6. When the customer is a legal person, a financial institution shall understand whether the customer is able to issue bearer shares and apply appropriate measures for customers who have issued bearer shares to ensure their beneficial owners are kept up-to-date. 7. When the customer is a legal person, an organization or a trustee, a financial institution shall, in accordance with Item (3) of Subparagraph 4 hereof, understand the ownership and control structure of the customer or the trust, and obtain the following information to identify the beneficial owners of the customer and take reasonable measures to verify the identity of such persons: (1) For legal persons and organizations: A. The identity of the natural person(s) who ultimately has a controlling ownership interest in
1	Examine whether the bank's internal rules and operating procedures include: ① How to identify and verify the beneficial owner(s) of a legal person customer, organization and trustee and verification methods (e.g. using public information to understand better or analyze the structure of a legal entity to confirm further its beneficial owner(s)). ② Scope of customer data to be collected using risk-based approach and how to identify and verify the beneficial owner(s) of a legal person customer, organization or trustee, and verification methods. ③Name screening to be performed on customers (including customer, its agent, beneficial owner or senior management) who apply for a new account. ④When the bank relies on a third	

No.	Examination Item	Legal Basis
	party to perform CDD, does the bank audit and monitor the third party's use, processing and control of customer information?	the legal person. A controlling ownership interest refers to owning directly and/or indirectly more than 25 percent of the legal person's shares or capital; a financial institution may ask the customer to provide its list of shareholders or other documents to assist in the identification of persons holding controlling ownership interest. B. To the extent where no natural person exerting control through ownership interests is identified under the preceding sub-item or that there is doubt as to whether the person(s) with the controlling ownership interest are the beneficial owner(s), the identity of the natural person(s) (if any) exercising control of the customer through other means. C. Where no natural person is identified under Sub-item A or B above, a financial institution shall identify the identity of a natural person who holds the position of senior managing official. (2) For trustees: the identity of the settlor(s), the trustee(s), the trust supervisor, the beneficiaries, and any other natural person(s) exercising ultimate effective control over the trust, or the identity of person(s) in equivalent or similar position. (3) Unless otherwise provided for in the proviso of Subparagraph 3,
2	Select a sample of high risk and more complex legal person customers to examine whether the CDD data on sampled customers saved by the bank are able to identify and verify the identity of beneficial owner, and whether there are scenarios where identification error has occurred or where the identification was correct but data filing was wrong.	

No.	Examination Item	Legal Basis
		Paragraph 1 of Article 6 or where the customer has issued bearer shares, a financial institution is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer set out under Item (3) of Subparagraph 4 hereof, provided the customer or the person having a controlling ownership interest in the customer is A. a R.O.C government entity; B. an enterprise owned by the R.O.C government; C. a foreign government entity; D. a public company and its subsidiaries; E. an entity listed on a stock exchange outside R.O.C. that is subject to regulatory disclosure requirements of its principal shareholders, and the subsidiaries of such entity; F. a financial institution supervised by the R.O.C. government, and an investment vehicles managed by such institution; G. a financial institution established outside R.O.C. that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the Financial Action Task Force on Money Laundering (FATF), and an investment vehicle managed by such institution; H. a fund administered by a R.O.C.

No.	Examination Item	Legal Basis
		government entity; or I. an employee stock ownership trust or an employee savings trust. (4) Except for situations provided for in the proviso of Subparagraph 3, Paragraph 1 of Article 6, a financial institution is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer set out under Item (3) of Subparagraph 4 hereof when the customer purchases property insurance, accident insurance, health insurance or an insurance product that does not require policy value reserve. 8. An insurance enterprise shall adopt the following measures when the beneficiary(ies) of a life insurance policy, investment related insurance policy or annuity insurance policy have been identified or designated: (1) Obtaining the name and identification document number or registration (incorporation) date of the designated beneficiary; and (2) For beneficiary(ies) that are designated by contract characteristics or by other means, obtaining sufficient information concerning the beneficiary to satisfy the insurance enterprise that it will be able to establish the identity of the beneficiary at the time of the payout.

No.	Examination Item	Legal Basis
		(3) Verifying the identity of the beneficiary(ies) at the time of the payout. 9. A financial institution shall not establish business relationship or conduct occasional transactions with a customer before completing the CDD measures. However, a financial institution may first obtain information on the identity of the customer and its beneficial owner(s) and complete verification after the establishment of business relationship, provided that: (1) The ML/TF risks are effectively managed, including adopting risk management procedures with respect to the conditions under which a customer may utilize the business relationship to complete a transaction prior to verification; (2) This is essential not to interrupt the normal conduct of business with the customer; and (3) Verification of the identities of the customer and its beneficial owner(s) will be completed as soon as reasonably practicable after the establishment of business relationship. A financial institution shall advise its customer in advance that the business relationship will be terminated if verification cannot be completed as soon as reasonably practicable. 」, Regulations Governing Anti-Money Laundering of Financial Institutions

No.	Examination Item	Legal Basis
		(December 14, 2021 Amended) , Financial Supervisory Commission 2.Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures & "Anti-Money Laundering and Anti-Terrorism Financing Guidelines for the Banking Sector (Template) and Related Regulations: Q&A for financial institutions
(C)	Name Screening	
1	Whether the bank establishes internal rules and operating procedures for risk-based name screening, which specify who should be subject to filtering, matching and filtering logic, implementation procedure for the filtering operation and evaluation standards.	1.Article 8「Financial institutions shall comply with the following provisions in their watch list filtering programs on customers and connected parties of transactions :1. A financial institution shall establish policies and procedures for watch list filtering, based on a risk-based approach, to detect, match and filter whether customers, or the senior managerial officers, beneficial owners or connected parties of the customers are individuals, legal persons or organizations sanctioned under the Terrorism Financing Prevention Act or terrorists or terrorist groups identified or investigated by a foreign government or an international organization.2. The policies and procedures for watch list filtering shall include at least matching

No.	Examination Item	Legal Basis
		and filtering logics, implementation procedures and evaluation standards, and shall be documented.3. A financial institution shall document its name and account filtering operations and maintain the records for a time period in accordance with Article 12.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission 2. Article 10 「When conducting CDD measures, a financial institution shall put in place risk management systems to determine whether a customer and its beneficial owner or senior managerial officer is a person who is or has been entrusted with a prominent function by a domestic government, a foreign government or an international organization (referred to as politically exposed persons (PEPs) hereunder)」 Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission
2	Does the bank use a risk-based approach to determine who should be subject to name screening procedure; those people should	The FSC's letter dated May 15,2016 to all supervised financial institutions「According to paragraph 311 of the Patriot Act, the US

No.	Examination Item	Legal Basis
	include at least the customers (including customers who purchase or use the products or services provided by the bank without a bank account; the same definition applies below), customer's senior management, and beneficial owner. The bank should identify additional objects to be screened using a risk-based approach and based on customer's ML/TF risk, which may include authorized signatories, customer's business, customer's major suppliers and major customers, issuing bank, beneficiary bank, decedent or donor from whom the customer receives the estate or gift, trust grantor, spouse, etc. If the account holder is a PEP, the screening should also cover the PEP's close associates.	Treasury Department has announced that North Korea is listed as a "mainly concerned country for money laundering"; the Ministry of Financial Crimes Inspection (FinCEN) also issued a notice to adopt specific measures to prohibit third-country banks from using the United States. The Correspondent Accounts deal with North Korean financial institutions and further isolate North Korea in the international financial system. Third, the case asks your Guild (social) to assist the members to pay attention to the relevant measures to be taken by the US Treasury Department to avoid being cut off by US financial institutions.」
3	Whether the bank specifies in its internal rules and operating procedures the test frequency, test items and methods for its name screening mechanism (including the appropriateness and effectiveness of match thresholds and filtering methods, accuracy and completeness of data creation and data output, etc.), and whether the bank conducts testing and save the track on testing. If the match threshold is set too low, it may result in a large number of false alerts, thereby increasing the operating costs of manual confirmation. But a match threshold	4th and 5th subparagraphs of Article 8 「4. The name screening mechanism should be subject to testing, including: (I) Whether the sanction list and threshold setting are determined by applying a risk-based approach. (II) Whether the mapping between data input and system data field is correct and complete. (III) The logic of matching and filtering. (IV) Model validation. (V) Whether data output is correct and complete. V. The bank should determine

No.	Examination Item	Legal Basis
	of 100% could lead to false negative and omission. Setting the match threshold too high or too low does not conform to the risk-based approach. The examiner should prudently evaluate bank's review of its threshold setting.	whether such mechanism continues to appropriately reflect the risk identified and update the mechanism at proper time.」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(approved by the FSC with letter dated April 23, 2019)，Bankers Association
4	Whether the bank has a mechanism for creating and updating sanction list and PEP (including the relatives of PEPs) list database and document relevant operating procedures, and whether the range and timeliness of database comply with the regulatory requirements.	
5	Whether the bank describes in its internal policy or rules and operating procedures for name screening the logic for matching and screening customer data, relevant transactions, or relevant accounts or locations, and how to obtain and update relevant lists in a timely manner, and the verification procedure for high-degree or potential matches identified in the screening results and actions to take (including how to investigate and confirm those matches and saving investigation documents for matches determined as false alert following verification, reporting procedure, etc.). For instance, if the result of name screening based on Romanization is 100% match or only the sequence of	

No.	Examination Item	Legal Basis
	last name and first name differs, inquire the sanction list to see if the date of birth matches.	
6	Whether the bank describes in its internal rules and operating procedures the procedures for handling account opening or transaction by customers (including their beneficial owners and other related parties as stipulated by law) who are designated on the sanction list or as a PEP, including but not limited to 1) decline to establish business relationship or carry out any transaction with individuals or organizations on the sanction list; 2) the operation for freezing the asset or property of sanctioned individuals or organizations and reporting procedure(refer to Appendix 5); and 3) adopt risk mitigating measures for high risk PEPs or PEPs with whom the business relationship is deemed high risk (for details, refer to "**Politically exposed persons**" under the section "**Effectiveness of internal controls**" of "**Policies and Procedures**").	1. 8th subparagraph of Article 4「The customer is an individual, a legal person or an organization sanctioned under the Terrorism Financing Prevention Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization, except for payments made under Subparagraphs 1 ~ 3, Paragraph 1, Article 6 of the Terrorism Financing Prevention Act」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission 2. 1st & 2nd paragraphs of Article 7「Except for the permission or restriction measures prescribed in Paragraphs 1 and 2 of preceding Article, the following acts shall be prohibited with respect to any designated individual, legal person, or entity under Paragraph 1 of Article 4 or of Article 5: 1. To make withdrawals, remittance, transfers, payment, deliveries or assignments related to financial accounts, currency or other payment instruments of the designated sanctioned individual, legal person and entity. 2. To make

No.	Examination Item	Legal Basis
		transfers, changes, dispositions, use of, or taking any other acts which may change the quantity, quality, value or location of any property or property interests of the designated sanctioned individual, legal person and entity. 3. To collect or provide any property or property interests for the designated sanctioned individual, legal person and entity. The provision of the preceding paragraph shall also apply to cases where a third party keeps or manages property or property interests of the designated individual, legal person and entity by authorization, appointment or trust of such individual, legal person and entity or due to other causes. An institution, business or profession prescribed in Paragraphs 1 to 3 of Article 5 of the Money Laundering Control Act shall immediately report any of the following circumstances discovered due to business relations to the Investigation Bureau of Ministry of Justice: 1. That institution, business or profession holds or manages property or property interests of an designated individual, legal person or entity. 2. Places where property or property interests of a designated individual, legal person or entity is

No.	Examination Item	Legal Basis
		located.」, Counter-Terrorism Financing Act, November 7, 2018 Amended, Ministry of Justice 3.The FSC's letter dated May 15,2016 to all supervised financial institutions「According to paragraph 311 of the Patriot Act, the US Treasury Department has announced that North Korea is listed as a "mainly concerned country for money laundering"; the Ministry of Financial Crimes Inspection (FinCEN) also issued a notice to adopt specific measures to prohibit third-country banks from using the United States. The Correspondent Accounts deal with North Korean financial institutions and further isolate North Korea in the international financial system. Third, the case asks your Guild (social) to assist the members to pay attention to the relevant measures to be taken by the US Treasury Department to avoid being cut off by US financial institutions.」.
7	Select samples based on the bank's risk assessment result, prior examination reports, and internal audit report to test the adequacy of the bank's watch list filtering operation: ①Make sampling heck high-risk new accounts (for any business) to examine whether the bank has conducted watch list filtering on	

No.	Examination Item	Legal Basis
	the customer and related parties before completing the account opening and retained relevant inquiry data. ②Make sampling check transactions that do not involve the account (including credit card and “walk-in” customers) to examine whether the bank has the incidence of conducting name screening after the transaction is completed, whether the bank saves filtering data, and whether the screening logic is consistent with the bank’s internal rules. ③Examine the records in the bank’s latest updated database to determine whether the time of update complies with its internal rules. If the bank uses information system to handle the name screening operation, determine whether the information system synchronously checks whether all of the bank’s existing customers and their beneficial owners as well as other related parties stipulated by laws and internal rules match any name in the updated database. If the examiner has question about the bank’s filtering and screening logic, he/she can input the names most recently added to the sanction list (or slightly modified name list) to test the effectiveness of the bank’s filtering and screening mechanism.	

No.	Examination Item	Legal Basis
	④ If the bank does not use information system in its watch listing filtering operation, examine whether the way by which the bank manually filters its existing customers is commensurate with the bank's risk profile. ⑤ Examine bank's cases of freezing customer asset or property to determine whether the bank handles the freeze operation (freeze, reporting and record-keeping) in accordance with relevant regulations and internal rules. ⑥ Identify the root causes of bank's deficiencies in name screening operation (e.g. inadequate training for staff handling the operation, poor internal controls, erroneous risk assessment, etc.) and give comments on those causes.	
(D)	Customer risk assessment and ongoing due diligence	
1	Whether the bank has established customer risk assessment methods and operating procedures, which should include at a minimum risk factors and risk levels, and whether the bank performs risk assessment in accordance with the operating procedures; the examiner should select samples to verify the bank's implementation status.	1st to 3th subparagraphs of Article 5「The CDD measures of a financial institution shall include ongoing customer due diligence and comply with the following provisions: 1. A financial institution shall apply CDD requirements to existing customers on the basis of materiality and risk, and conduct due diligence on such existing relationships at appropriate times, taking into
2	Whether the bank has established internal rules and operating	

No.	Examination Item	Legal Basis
	procedures for the time for ongoing due diligence and updating customer data based on the investigation results, and performed ongoing due diligence accordingly; the examiner can select and examine recently opened bank accounts, or credit, trust, or e-payment accounts of existing customers, or legal person customers with responsible person changed, or customers with nationality changed. If it is found that considerable time has elapsed since due diligence was last performed on a customer, the examiner should check if due diligence and risk assessment were performed when the customer added any of the aforementioned business relationships.	account whether and when CDD measures have previously been undertaken and the adequacy of data obtained. The aforementioned appropriate times shall include at least: (1) When the customer opens another new account, registers another new stored value card, registers another new e-payment account, increases the amount insured irregularly or enters new business relationships with the financial institution; (2) When it is time for periodic review of the customer scheduled on the basis of materiality and risk; and (3) When it becomes known that there is a material change to customer's identity and background information. 2. A financial institution shall conduct ongoing due diligence on the business relationship to scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, its business and risk profile, including, where necessary, the source of funds. 3. A financial institution shall periodically review the existing customer records to ensure that documents, data or information of

No.	Examination Item	Legal Basis
		the customer and its beneficial owner(s) collected under the CDD process are adequate and kept up-to-date, particularly for higher risk categories of customers, whose reviews shall be conducted at least once every year.」, Regulations Governing Anti-Money Laundering of Financial Institutions Designated (December 14, 2021 Amended), Financial Supervisory Commission
3	Whether the bank has established the mechanism for inspecting the adequacy of information (including information on beneficial owners) obtained in CDD and whether the bank has performed the inspection accordingly. The examiner should check the risk factors set by the bank in its customer risk assessment operation against the CDD information actually obtained by the bank (preferably the CDD information of high-risk customers) to examine whether the CDD information is sufficient to support its risk assessment result. In addition, the examiner should select a sample of existing high-risk customers who carry out new transactions to examine whether there is change to the customer's beneficial owner but the bank did not update such information in the latest update.	
4	Whether the bank sets the frequency of reassessing the risk of customers at different risk levels, and except for	

No.	Examination Item	Legal Basis
	high-risk customers, is the bank's frequency of risk reassessment for customers at other risk levels commensurate with the bank's aggregate risk profile.	
5	Whether the bank adjusts the risk level of customers based on the results of ongoing monitoring.	
(E)	Enhanced due diligence (EDD)	
1	Whether the bank has established internal policy or rules and operating procedures for EDD for high-risk customers (customers who are identified as high risk based on the bank's risk assessment result, bank policies and FSC regulations), and the EDD measures at least are not below the standards set forth by the FSC and the Bankers Association.	1. 1st paragraph of Article 6「A financial institution shall determine the extent of applying CDD and ongoing due diligence measures under Subparagraph 4 of Article 3 and the preceding article using a risk-based approach (RBA): 1. For higher risk circumstances, a financial institution shall perform enhanced CDD or ongoing due diligence measures by adopting additionally at least the following enhanced measures: (1) Obtaining the approval of senior management before establishing or entering a new business relationship; (2) Taking reasonable measures to understand the sources of wealth and the source of funds of the customer; in case the source of funds is deposits, understand further the source of deposits; and (3) Conducting enhanced ongoing monitoring of business relationship.
2	Screen high-risk customers who just enter business relationship with the bank to examine whether the bank performs EDD on those customers in accordance with its internal rules.	

No.	Examination Item	Legal Basis
		2. For customers from high ML/TF risk countries or regions, a financial institution shall conduct enhanced CDD measures consistent with the risks identified. 3. For lower risk circumstances, a financial institution may apply simplified CDD measures, which shall be commensurate with the lower risk factors. However simplified CDD measures are not allowed in any of the following circumstances: (1) Where the customers are from or in countries and jurisdictions known to have inadequate AML/CFT regimes, including but not limited to those which designated by international organizations on AML/CFT as countries or regions with serious deficiencies in their AML/CFT regime , and other countries or regions that do not or insufficiently comply with the recommendations of international organizations on AML/CFT as forwarded by the Financial Supervisory Commission(FSC); or (2) Where there is a suspicion of money laundering or terrorist financing in relation to the customer or the transaction. The provisions of Items (1) and (2) of Subparagraph 1 of the

No.	Examination Item	Legal Basis
		preceding paragraph do not apply to electronic stored value card registration operation. 」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission 2.5th subparagraph and 9th subparagraph of Article 4「V. For an individual customer that is identified by a bank as a high-risk customer or a customer that has certain high-risk factors in accordance with the bank's relevant requirements on customer ML/TF risk assessment, the bank should obtain at least any of the following information when establishing business relationship: (i)Any other names used or alias: such as the name used before marriage or change of name; (ii)Employer's address, post office box address, e-mail address (if any); or (iii) Landline or mobile telephone numbers. IX. For a customer identified by a bank as a high-risk customer or a customer that has certain high-risk factors in accordance with the bank's relevant requirements on customer ML/TF risk assessment, the bank should

No.	Examination Item	Legal Basis
		perform enhanced verification, for example: (i) Obtaining a reply, signed by the customer or the authorized signatory of the entity, for a letter mailed to the address provided by the customer, or contacting the customer by telephone. (ii)Obtaining evidence that supports an individual's sources of wealth and sources of funds. (iii)Obtaining evidence that supports the sources of funds and destinations of funds of an entity or trustee of a trust, such as a list of main suppliers, a list of main customers, etc.(iV) Site visit. (V)Obtaining prior bank reference and contacting with the bank regarding the customer.」,Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association
(F)	Political exposed persons (PEP) (With regard to "**Risk factors**", "**Risk mitigating measures" and "Examination Items"), refer to "Politically exposed persons"** under the section "**Effectiveness of internal controls**" of "**Policies and**	

No.	Examination Item	Legal Basis
	Procedures”).	
(G)	Decline to establish business relationship with customer	Article 4「If there exists any of the following situations in the CDD process, a financial institution should decline to establish business relationship or carry out any transaction with the customer:
1	Whether the bank has established internal policy or rules and operating procedures for declining to establish business relationship with certain customers.	1. The customer is suspected of opening an anonymous account or using a fake name, a nominee, a shell firm, or a shell corporation or entity to open an account, purchase insurance or register an electronic stored value card;
2	Examine the bank’s cases of declining to establish business relationship with customer to evaluate whether the bank had adequate reason to turn down a customer and has done so in a timely manner, and whether the bank saves adequate information thereon.	2. The customer refuses to provide the required documents for identifying and verifying its identity; 3. Whereas any person acts on behalf of a customer to open an account, register an electronic stored value card, register an e-payment account, apply for insurance, file an insurance claim, request change of insurance contract or conduct a transaction, it is difficult to check and verify the fact of authorization and identity-related information; 4. The customer uses forged or altered identification documents; 5. The customer only provides photocopies of the identification documents; the preceding provision does not apply to businesses where a photocopy or image file of the identification document supplemented with other control

No.	Examination Item	Legal Basis
		measures are acceptable; 6. Documents provided by the customer are suspicious or unclear so that the documents cannot be authenticated, or the customer refuses to provide other supporting documents; 7. The customer procrastinates in providing identification documents in an unusual manner; 8. The customer is an individual, a legal person or an organization sanctioned under the Terrorism Financing Prevention Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization, except for payments made under Subparagraphs 1 ~ 3, Paragraph 1, Article 6 of the Terrorism Financing Prevention Act; or 9. Other unusual circumstances exist in the process of establishing business relationship or conducting transaction and the customer fails to provide reasonable explanations.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission
C	**Ongoing Monitoring and Filing of Suspicious Transaction Reports(STR)**	
(A)	Whether the bank has selected or developed suitable red flags based on its size of assets, geographic locations, business profile, customer	

No.	Examination Item	Legal Basis
	base profile, characteristics of transactions, and in reference to the bank's internal ML/TF risk assessment or information of daily transactions, and based on which, established an effective system for ongoing monitoring of accounts and transactions. When evaluating the effectiveness of the bank's monitoring system, the examiner should consider the bank's aggregate risk profile (high risk products, services, customers, delivery channels and geographic locations), volume of transactions and adequacy of manpower allocation.	
1	The bank can carry out its monitoring operation by way of manual identification, information system or a combination of both. If the bank identifies alerts or suspicious transactions manually, the examiner should determine whether the bank has allocated adequate manpower to carry out the AML/CFT operation effectively.	1.1st subparagraph to 5th subparagraph of Article 9 「Financial institutions shall observe the following provisions for ongoing monitoring of accounts or transactions: 1. A financial institution shall use a database to consolidate basic information and transaction information on all customers for
2	Whether the bank posts data and information obtained in customer due diligence process (including EDD) completely into its information system to facilitate the monitoring and analysis of customer accounts and transactions. The examiner should make sampling check the CDD and EDD data of high-risk customers to determine whether information that aids in the analysis of ML/TF	inquiries by the head office and branches for AML/CFT purpose so as to strengthen the institution's capability of account and transaction monitoring. A financial institution shall also establish internal control procedures for requests and inquiries as to customer information made by various units and shall exercise care to ensure the confidentiality

No.	Examination Item	Legal Basis
	risks has been completely posted or captured in the information system.	of the information.
3	Whether the bank has established policies and procedures (i.e. internal rules and operating procedures) for account and transaction monitoring, which should include confidentiality mechanism for customer data obtained by relevant bank units in the investigation, customer account or transaction monitoring operation (including complete monitoring patterns, parameter setting and threshold amounts), procedure for suspicious transaction (including alert cases) monitoring operation and procedure for investigating monitored cases (including the units that should carry out investigation, items to be investigated, supporting evidence to be attached, and standards for report examination) and reporting standards, and whether the bank has established internal rules and operating procedures for confidentiality mechanism for suspicious transactions reported, update mechanism for account and transaction monitoring policies and procedures (including division of labor and responsibilities of relevant units and staff).	2. A financial institution shall establish policies and procedures for account and transaction monitoring using a risk-based approach and utilize information system to assist in the detection of suspicious ML/TF transactions. 3. A financial institution shall review its 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. 4. The policies and procedures for account and transaction monitoring of a financial institution shall 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, and shall be documented.
4	The examiner should select a sample of high-risk customers who recently have credit dealing with the bank or open a trust account or apply for	5. Complete ML/TF monitoring indicators mentioned in the preceding subparagraph shall, based on the business nature of the financial institution, include

No.	Examination Item	Legal Basis
	credit card to examine if the basic data of the same customer in different product systems have any inconsistency and if the basic data and transaction data of the same customer (e.g. occupation, business operated, or line of business, address and financial condition) in different product systems differ from the data in the integrated system to verify whether the bank integrates customer data.	the suspicious indicators published by the trade associations and the additional ones developed by the financial institution in reference to its ML/TF risk assessment or daily transaction information. With regard to transfer of funds between e-payment accounts, a financial institution should, when carrying out the monitoring, take into consideration all information received on both accounts to determine whether to file a suspicious ML/TF transaction report.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission 2. Employed personnel prescribed in paragraphs 1 to 3 of Article 5, who are not public officials, and who disclose or deliver documents, pictures, information or objects relating to reported transactions suspected of violating provisions under Articles 14 and 15, or to suspected offences described in Articles 14 and 15, will f shall be sentenced to imprisonment of not more than two year, a detention, or a fine of not more than NT$500,000.」, Money laundering Act, amended on November 7, 2018, Ministry of Justice 3.3rd subparagraph and 4th

No.	Examination Item	Legal Basis
		subparagraph of Article 9 「III.The bank should review its policies and procedures for ongoing monitoring of accounts and transactions and update periodically to take into account regulatory requirements on AML/CFT, customer profiles, the size and complexity of business, the trend and information related to ML/TF obtained from internal or external sources, the result of internal risk assessment, etc. IV. Policies and procedures for ongoing monitoring of accounts and transactions should include at least complete and documented monitoring types, parameters, thresholds, operating procedures for the conducting and monitoring of alerts, procedures for reviewing monitoring cases, and the standard of reporting.」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association
(B)	Whether the bank has established internal rules and operating procedures for identifying, investigation and reporting suspicious transactions (including alerts), and whether reports outputted from the information monitoring system cover comprehensively red flags of suspicious transactions set by the bank and high-risk customers, high-risk products and services, and transactions involving high-risk areas	

No.	Examination Item	Legal Basis
	identified.	
1	Whether the bank has developed red flags of money laundering or terrorist financing using a risk-based approach, and based on which, determine the setting of relevant parameters or screening indicators. The examiner can refer to the Annex "Red Flags for Suspicious Money Laundering or Terrorism Financing Transactions" of the "Template of Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism of Bank." However it should be noted that the red flags listed in the Annex are not mandatory that the bank may determine on its own red flags to be included based on its risk assessment result. For more complex products and services, products that come in a wide variety and provided by multiple branches (or subsidiaries) or products and services offered to a diverse customer base, the bank may need to develop more refined indicators.	Annex: Red Flags for Transactions Suspected to Involve Money Laundering or Terrorism Financing, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association
2	The identification of some suspicious ML/TF transactions may need to rely on frontline bank staff (e.g. several individuals show up together at the bank to carry out deposit, withdrawal or wire transfer transactions, lacking reasonable information of the underlying trade's quantities and prices in the transactions of issuing letters of credit that accumulatively	1.9th subparagraph, 1st paragraph of Article 9「With respect to red flags for transactions suspected to involve money laundering or terrorism financing, the bank should determine the ones that are required to be monitored with the assistance of related information systems by applying a risk-based approach. For those that are

No.	Examination Item	Legal Basis
	reach a specific amount, an originator of cross-border wire transfer fails to provide a reasonable explanation on the relationship between the originator and the beneficiary, the customer engages in a transaction for which customer identification process cannot be completed, a customer opens his/her safe deposit box with several other individuals, and other red flags associated with customer behaviors); whether the bank provides adequate job or business related training to its employees and has established relevant internal rules and operating procedures for observance by employees, for example, signs of suspicious ML/TF transactions, how a bank employee handles customer transaction without tipping off the customer that his transaction is suspected of money laundering or terrorist financing, and a STR must be filed regardless whether the suspicious transaction is completed or not, and the procedures for reporting to the dedicated compliance unit.	monitored without the assistance of information systems, the bank should also, by other means, assist employees to determine whether transactions are suspicious ML/TF transactions when they are processed by customers. The assistance of information system cannot replace the judgment of employees. The bank is still required to strengthen employee training to allow employees capable of identifying suspicious ML/TF transactions.」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association 2.2nd paragraph of Article 9「Reporting of suspicious ML/TF transactions: I. When an employee of a business unit identifies any abnormal transaction, the employee should immediately report such transaction to a supervisory officer. II.The supervisory officer should determine as soon as possible whether such transaction is subject to reporting requirements. If it is determined that such transaction should be reported, the

No.	Examination Item	Legal Basis
		supervisory officer should immediate request the employee complete a report (please download the reporting format on the website of the Investigation of Bureau, Ministry of Justice). III. After the report is approved by the head of the business unit, the bank should submit the report to the responsible unit. IV. After the report is submitted by the responsible unit and approved by AML/CFT Responsible Officer, the bank should file the report immediately to the Investigation of Bureau, Ministry of Justice. V. In the case of an apparently significant and urgent suspicious ML/TF transaction, the bank should immediately report to the Investigation of Bureau, Ministry of Justice by fax or other feasible means and then immediately submit the hard copy of the report. The bank is not required to submit the hard copy of the report, provided that the Investigation of Bureau, Ministry of Justice confirms the receipt of such report by sending a fax reply (please download the format on the website of the Investigation of Bureau, Ministry of Justice. In

No.	Examination Item	Legal Basis
		addition, the bank should retain the fax reply. 」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association
3	For suspicious ML/TF transaction cases under investigation named in the correspondence from a law enforcement agency, the bank should have internal rules and operating procedures for handling this kind of cases, which should preferably include: confidentiality mechanism for relevant cases, reporting to the dedicated compliance unit for investigating suspicious transactions, etc. The bank should also judge, based on the customer information at hand and investigation result, whether to file a STR and should not determine directly that the customer is involved in a ML/TF transaction based solely on the ground that the transaction is being investigated by the law enforcement agency.	
4	The examiner should ask the bank to provide independent testing report, records or descriptions on its account and transaction monitoring mechanism (including whether the logic of setting parameters or filtering indicators is commensurate	5th subparagraph, 1st paragraph of Article 9「V. The mechanism provided in last subparagraph should be subject to testing, including: (i)Internal control procedure: review the roles and responsibilities of persons or business units related to

No.	Examination Item	Legal Basis
	with the bank's ML/TF risk profile) and examine whether the testing scope is comprehensive. The examiner can also select a sample of high-risk customers or products and services to verify whether the bank's account and transaction monitoring mechanism is consistent with its documented rules and operating procedures. The verification should cover at least the actual internal control process, whether data stored in the system are consistent with customer's CDD (including EDD) and complete or whether there are errors in the data entry fields, and whether transactions that match the bank-set parameters or filtering indicators are included in related reports to verify whether parameters or filtering indicators set in the system are the same as those specified in the bank's documented rules, and whether access authority of the monitoring system is properly set, in particular whether the change of parameter is subject to proper internal check.	the mechanism for monitoring accounts and transactions. (ii)Whether the mapping between data input and system data field is correct and complete. (iii)The logic of detection scenario. (iv)Model validation. (v)Data input.」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association
5	With regard to the testing of ongoing monitoring mechanism for accounts and transactions mentioned in the preceding paragraph, the examiner should confirm the suitability of testing unit that except for manual monitoring, testing should be performed by the head office if the design of ongoing monitoring mechanism throughout the bank is	Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures & "Anti-Money Laundering and Anti-Terrorism Financing Guidelines for the Banking Sector (Template) and Related Regulations: Q&A for financial institutions

No.	Examination Item	Legal Basis
	identical. If part of the monitoring mechanism of an overseas branch differs from that of the head office, the overseas branch should test that part on its own. The examiner should also check the inspection report and internal audit report produced by the overseas branch to determine whether the design of ongoing monitoring mechanism of the overseas branch is the same as that of the head office.	
(C)	Whether the bank's investigation, evaluation and handling of identified suspicious transactions (including alert cases) are appropriate.	
1	Determine whether the bank has internal rules and operating procedures in place to ensure that the information monitoring system is capable of generating a suspicious transactions statement in a timely manner and to require the checking, analysis and investigation of outputted suspicious transactions, and whether the bank has a mechanism to ensure that suspicious transactions (regardless whether the transaction is completed or not) identified by bank employees in daily operations or investigated by a law enforcement agency as indicated in its correspondence to the bank are all included in the scope of investigation and evaluation.	
2	Determine whether the bank has allocated adequate manpower to	

No.	Examination Item	Legal Basis
	inspect suspicious transactions statement and make investigation, and whether relevant employees have the skills required to conduct an investigation and are equipped with adequate tools. For example, does the investigator have sufficient system access authority to inquire all basic data or transaction records of a customer, are all CDD and EDD data of customers keyed into the system, and whether the system can retrieve all transactions of a customer taken place during a period of time.	
3	Whether the bank has the practice of adjusting parameters or filtering indicators in coordination with its current manpower or other factors to decrease the number of suspicious transactions or transaction alerts that the information monitoring system can output, thereby undermining the effectiveness of the bank's AML/CFT program. Below are a few examples of the methods for verifying effectiveness: (1) Select a sample of high-risk customers based on the bank's risk assessment result (data on high-risk customers, products or services), prior examination reports, bank's internal audit report and correspondence from law enforcement agencies regarding investigation of customers who may be involved in a ML/TF transaction, and	

No.	Examination Item	Legal Basis
	peruse their account opening data, customer review data (CDD and EDD), all transactions during a period of time (deposit/withdrawal, wire transfer, lending, etc.) or relevant files on credit extension. (2) After checking relevant data, the examiner should select a sample of suspicious transactions to see if the nature of transaction is consistent with the customer's CDD information (e.g. occupation, expected transactions, sources of fund of individual customers, or the business of the legal entity, size of business, business location and major markets, etc.). If there is any inconsistency, the examiner should discuss with responsible management to see if a suspicious transaction has a reasonable explanation, and based on the explanation, determine whether the bank has failed to output reportable suspicious transactions and whether the bank's information monitoring system is able to effectively detect suspicious transactions. If the examiner has doubt about the system's effectiveness, he/she should understand the causes (e.g. improperly set screening indicators, inadequate risk	

No.	Examination Item	Legal Basis
	assessment, or error in the judgment of chief AML/CFT compliance officer), and describe the findings in the examination report. (3) Verify the effectiveness of the bank's screening of existing customers whether a customer is an individual, a legal person or an organization sanctioned under the Terrorism Financing Prevention Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international organization. For details, see examination items under the section "name screening".	
4	Whether the bank has internal rules and operating procedures in place for analysis, investigation, reporting and follow-up of suspicious transactions, which should include at a minimum: 1) the chief AML/CFT compliance officer gives the final review as to whether to file a STR with the Investigation Bureau, Ministry of Justice; 2) Written analysis and reasons for deciding not to file a STR; 3) supporting evidence to be investigated and attached; 4) actions to be taken on a customer whose transactions have been reported as suspicious several times (e.g. ending the business relationship with the customer), and the chief AML/CFT compliance officer is	

No.	Examination Item	Legal Basis
	responsible for supervising the follow-up after a STR is filed.	
5	When verifying the bank's handling of suspicious transactions, the examiner should determine whether the bank makes judgment on the reasonableness of a customer's transaction based on all available customer review information (CDD and EDD), whether there is a written analysis sufficient to support the final decision on a suspicious transaction (to file or not to file a STR), and regardless whether a transaction is determined to be a suspicious transaction or not, does the bank retain the records on analysis and judgment made and supporting data.	1.6th subparagraph, 1st paragraph of Article 9「 Financial institutions shall observe the following provisions for ongoing monitoring of accounts or transactions: 6. A financial institution shall document its ongoing account and transaction monitoring operation and maintain the records in accordance with Article 12 herein. 」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission 2.8th subparagraph, 1st paragraph of Article 9「VIII. For red flag transactions identified in accordance with last subparagraph, the bank should determine whether such transactions are reasonable (e.g. whether such transactions are apparently incommensurate with the identity, income, or scale of business of the customer, unrelated to the customer's business profile, do not match the customer's business model, no reasonable economic purpose, no reasonable explanation, no reasonable purpose, or unclear source of funds or explanation),

No.	Examination Item	Legal Basis
		the bank shall complete the review process as quickly as possible to determine whether the transaction is suspected of involving ML/TF activity, and keep review records. If the bank examines and determines such transaction is not a suspicious ML/TF transaction, the bank should record the reason for the decision. If the bank examines and determines such transaction is a suspicious ML/TF transaction, regardless of the amount of the transaction, the bank shall promptly file a report with the Investigation Bureau in a format prescribed by the Bureau after the report has been approved by the responsible chief compliance officer at the bank. The same process shall apply to attempted transactions..」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association 3.16th subparagraph, 1st paragraph of Article 4「XVI. In the case that a customer in a business

No.	Examination Item	Legal Basis
		relationship or transaction is described in subparagraph I.(viii), a bank should report suspicious ML/TF transaction in accordance with Article 10 of Money Laundering Control Act. If such customer is a designated individual or entity sanctioned under Counter-Terrorism Financing Act, the bank is prohibited from the activities described in paragraph 1 of Article 7 of Counter-Terrorism Financing Act since the date of knowledge, and should report in accordance with the requirements of Counter-Terrorism Financing Act (please download the reporting format on the website of the Investigation Bureau, Ministry of Justice)」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association 4. 8th item, 1th subparagraph, 1st paragraph of Article 4「(viii)The parties with whom a bank establishes business relationship are designated individuals or

No.	Examination Item	Legal Basis
		entities sanctioned under Counter-Terrorism Financing Act and terrorists or terrorist groups that are identified or investigated. This requirement, however, does not apply to any payment made in accordance with subparagraph II to IV of paragraph 1 of Article 6 of "Counter-Terrorism Financing Act」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association 5.Regulations Governing Reporting on the Properties or Property Interests and Locations of Designated Sanctioned Individuals or Entities by Financial Institutions (November 14 ,2018 Amended) , Financial Supervisory Commission
6	Whether a bank files a STR or not is partly predicated on the subjective judgment of the AML/CFT compliance officer and unit. Thus the examiner should put the focus on whether the bank has established an effective judging and investigation mechanism. Unless the bank's failure to file a STR following analysis and investigation involves gross	

No.	Examination Item	Legal Basis
	negligence or the supporting data are apparently erroneous that affects the analysis and judgment of AML/CFT compliance officer and unit, the examiner should not criticize the subjective judgment made by them.	
7	When the bank detects and confirms internally a suspicious transaction (including scenarios where the inability to complete the CDD process on a customer leads the bank to suspect ML/TF activities, or if a bank forms a suspicion of money laundering or terrorist financing and reasonably believes that performing the CDD process will tip-off the customer, it is permitted not to pursue that process and file an STR instead), does the bank file a report to the Investigation Bureau, Ministry of Justice within 10 business days.	Article 15 「Financial institutions shall file suspicious ML/TF transaction reports in accordance with following provisions: 1. For transactions related to the monitoring patterns under Subparagraph 5 of Article 9 herein or other situations that are deemed as suspicious ML/TF activities, a financial institution shall file a suspicious transaction report (STR)with the Investigation Bureau, regardless of the amount of transaction and regardless whether the transaction was completed or not. 2. Within ten (10) business days upon discovery of a suspicious ML/TF transaction, a financial institution shall promptly file a STR with the Investigation Bureau in a format prescribed by the Bureau after the report has been approved by the responsible chief compliance officer at the institution. 3. For obviously significant suspicious ML/TF transactions of urgent nature, a financial institution should file a report as soon as possible to the Investigation Bureau by fax or other available means and

No.	Examination Item	Legal Basis
		follow it up with a written report. The financial institution is not required to submit a follow-up written report, provided the Investigation Bureau has acknowledged the receipt of report by sending a reply by fax. In such event, the financial institution shall retain the faxed reply. 4. The formats of STR and faxed reply mentioned in the preceding two subparagraphs shall be prescribed by the Investigation Bureau. 5. The data reported to the Investigation Bureau and relevant transaction records shall be kept in accordance with Article 12 herein.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended), Financial Supervisory Commission
(D) 1	Whether the bank files cash transaction reports (CTR) according to rules. The examiner should make sampling check based on the bank's risk assessment result, prior examination reports, internal audit report and verification report on related information system to understand deficiencies in the bank's CTR operation, make sampling check control weakness, and confirm the manner by which the bank outputs reportable large cash transaction	1. Article 13「Financial institutions shall 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 following provisions: (1) Check the identity (ID)

No.	Examination Item	Legal Basis
	data.	document or passport provided
2	If the bank system uses automated large cash transactions reporting, the examiner should examine whether the system's screening logic has any omission. For example, are cash transactions screened by customer account numbers only that large cash payments on credit card debt or large cash deposits into the bank's escrow account are missed, or are non-business related frequent or routine large cash deposits made by customers in some lines of business,	by the customer and record the customer's name, date of birth, address, telephone, account number, amount of transaction, and ID number. Notwithstanding the foregoing, in case that the customer is confirmed to be exactly the accountholder, it should be clearly noted in the transaction record rather than undertaking a repeated ID verification.
3	such as department store and supermarkets excluded from the reporting scope. If the examiner finds omissions, he/she should understand the reasons and make pertinent comments in the examination report.	(2) If the transaction is conducted by an agent, check the identity of the agent by checking his or her ID document or passport and record the name, date of birth, address, and telephone of the agent, account number, amount of transaction, and ID number.
	If the bank relies on system output of all large cash transactions and then manually picks reportable transactions, the examiner should make sampling check transactions taken place during a period of time to determine whether the manually picked non-individual accounts which need not be reported are all accounts of department stores, supermarkets, gas stations, hospitals, transportation businesses and restaurants and hotels that are on a list the bank has sent to the Investigation Bureau for record, and determine whether the bank has established an internal control mechanism to ensure the	(3)For occasional transactions, verify the identity of the customer in accordance with Paragraph 4of Article 3 herein. 3. Except for situations specified in Article 14 herein, report the transaction to the Investigation Bureau, Ministry of Justice(referred to as "Investigation Bureau" hereunder) in a format prescribed by the Investigation Bureau via electronic media in five(5)business days after the completion of transaction. If a

No.	Examination Item	Legal Basis
	accuracy of manual pick operation.	financial institution is unable to file a report via electronic media with a legitimate reason, the institution may file a written report after obtaining the consent of the Investigation Bureau.
4	Does the bank have the situation of reporting a large cash transaction late? If there is, the examiner should understand the reasons and make pertinent comments in the examination report.	4. Keep the data reported to the Investigation Bureau and relevant transaction records in accordance with Article 12 herein.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission 2. Article 14「A financial institution is not required to file a report on any of the following cash transactions above a certain amount with the Investigation Bureau, provided the financial institution verifies the identity of the customer and keeps the transaction records thereof: 1. Deposits into the accounts opened by government agencies, state-run enterprises, institutions acting with governmental power (within the scope of mandate), public and private schools, public enterprises and government funds established where relevant regulations or contractual relationships so provide. 2. Receivables and payables collected and made by a financial

No.	Examination Item	Legal Basis
		institution on behalf of government treasuries. 3. Transactions and fund arrangements between financial institutions. Notwithstanding the foregoing, payables to another financial institution's customer paid through an inter-bank deposit account, such as a customer cashing the check issued by another financial institution, shall be handled as required, provided the cash transaction of the same customer exceeds a certain amount. 4. Funds paid by a lottery merchant for purchasing lottery tickets. 5. Payments collected on behalf of a third party (excluding payments deposited in designated stock subscription accounts and credit card payments collected) where the payment notice expressly bears the name and ID Card number of the counterparty (including the code which enables tracking of counterparty's identity), and type and amount of transaction. Nevertheless, the duplicate copy of the payment notice shall be kept as the transaction record. In case of non-individual accounts such as those opened by department stores, megastores, supermarket chains, gas stations, hospitals, transportation businesses and

No.	Examination Item	Legal Basis
		hotels and restaurants which must deposit cash amounting to over a certain amount constantly or routinely in line with business needs, a financial institution may, after verifying the actual business needs, submit the name list to the Investigation Bureau for recordation. Verification and reporting of transactions on a case-by-case basis may be waived for such an account unless the Investigation Bureau responds to the contrary within ten (10) days from the receipt of the name list. A financial institution shall examine the counterparties to the transactions exempted from reporting on a case-by-case basis at least once every year, and report to the Investigation Bureau for recordation if a counterparty no longer has business dealing as mentioned in this paragraph with it.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended), Financial Supervisory Commission
D	**Policies and Procedures**	
(A)	AML/CFT program	
1	Whether the bank has documented anti-money laundering and countering the financing of terrorism (AML/CFT) program (including internal rules and operating procedures relating to AML/CFT),	1.1st paragraph of Article 6「The AML/CFT internal control system established by a banking business, electronic payment institution or electronic stored value card issuer and any subsequent amendment

No.	Examination Item	Legal Basis
	which requires the board of directors and chief AML/CFT compliance officer to take charge of monitoring and controlling AML/CFT risks and the AML/CFT program has been passed by the board of directors; whether the bank periodically examines the necessity of updating its AML/CFT program and adopts the same approval hierarchy and procedure for the establishment and update of AML/CFT program.	thereto shall be approved by its board of directors (council)」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission 2. 2nd paragraph of Article 7「The dedicated AML/CFT compliance unit or the chief AML/CFT compliance officer mentioned in the preceding paragraph shall be charged with the 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 company-wide AML/CFT risk identification and assessment. 3. Monitoring and controlling ML/TF risks.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
2	Whether the relevant policies, procedures or documented internal rules (e.g. instructions, measures, guidelines, etc.) established by the	3rd paragraph of Article 6「The AML/CFT program mentioned in Subparagraph 2 of Paragraph 1 hereof shall include the following

No.	Examination Item	Legal Basis
	bank cover customer due diligence (including verification of customer identity and name screening), record keeping, reporting of cash transactions above a certain amount, reporting of transactions suspicious of AML/CFT, matters that chief AML/CFT compliance officer is in charge of (including responsibilities of the chief compliance officer and dedicated compliance unit), AML/CFT management framework, including important issues or reports that should be presented to the board of directors and parent bank or head office (e.g. overall risk assessment result, risk prevention program and major suspicious transactions, etc.), employee screening and hiring procedure, ongoing employee training plan, independent audit function for testing the effectiveness of AML/CFT system, overall AML/CFT risk and risk mitigating measures (including ongoing monitoring of correspondent bank accounts and transactions).	policies, procedures and controls: 1. Customer due diligence; 2. Watch list filtering; 3. Ongoing due diligence 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. Employee screening and hiring procedure; 10. Ongoing employee training program; 11. An independent audit function to test the effectiveness of AML/CFT system; and 12. Other matters required by the AML/CFT regulations and the FSC.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
3	Whether the bank's relevant unit reports non-compliance with internal AML/CFT related rules or operating procedures or major deficiencies (including deficiencies of the	1.3rd paragraph of Article 7 「The chief AML/CFT compliance officer mentioned in Paragraph 1 hereof shall report to the board of directors (council) and supervisors (board of

No.	Examination Item	Legal Basis
	overseas branches) or major events (e.g. changes of domestic or foreign laws and regulations) that affect the effectiveness of anti-money laundering to the board of directors and senior management in a timely manner, analyzes causes and proposes improvement plan (including whether it is necessary to revise the AML/CFT program); if a major regulatory violation is discovered, the chief AML/CFT compliance officer shall promptly report to the board of directors and supervisors or the audit committee.	supervisors) or the audit committee at least semiannually, or whenever a major regulatory violation is discovered.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission 2. 6th paragraph of Article 6 「The board of directors (council) of a banking business and other financial institutions designated by the FSC takes the ultimate responsibility of ensuring the establishment and maintenance of appropriate and effective AML/CFT internal controls. The board of directors (council) and senior management of a banking business and other financial institutions designated by the FSC shall understand the company's ML/TF risks and the operation of its AML/CFT program, and adopt measures to create a culture of AML/CFT compliance.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
4	Whether the board of directors and	

No.	Examination Item	Legal Basis
	senior management require the chief AML/CFT compliance officer to report to them the implementation status and outcome of AML/CFT program (including but not limited to cases of AML related regulatory violation, improvement actions taken and the effectiveness of AML/CFT program) at least semi-annually, and whether the report presented is complete.	
5	Do the bank's internal rules and operating procedures specify the frequency by which the dedicated AML/CFT compliance unit and/or internal audit unit should report to the board of directors and senior management, and has the compliance unit made report according to the established frequency?	
6	Do the senior manager of legal compliance unit and the compliance officers of all business units have adequate independence, powers, channels and resources to effectively perform their AML/CFT duties?	
7	Do bank's directors, supervisors and president receive a set number of hours of training on AML/CFT every year, and whether the training covers topics in relation to their duties, for example, letting board members realize that the board of directors shoulders the ultimate responsibility for establishing and maintaining proper and effective AML/CFT	1.5th paragraph of Article 9 「A banking business and other financial institutions designated by the FSC shall annually arrange appropriate hours and contents of orientation and on-the-job training on AML/CFT for its directors (council members), supervisors, president, legal compliance personnel, internal auditors, and business personnel in

No.	Examination Item	Legal Basis
	internal controls and letting board members sufficiently understand the contents and meaning of AML/CFT report; has relevant members signed and issued a statement on internal AML/CFT controls?	view of the nature of its business, to familiarize them with their AML/CFT duties and equip them with the professional knowhow to perform their duties.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission 2. 3rd paragraph of Article 8「The president of a banking business and other financial institutions designated by the FSC shall oversee the respective units to prudently evaluate and review the implementation of internal control system for AML/CFT. The chairman, president, chief auditor and chief AML/CFT compliance officer shall jointly issue a statement on internal control for AML/CFT (see attached), which shall be submitted to the board of directors (council) for approval and disclosed on their website of the business and institutions within three (3) months after the end of each fiscal year, and filed via a website designated by the FSC.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other

No.	Examination Item	Legal Basis
		Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
8	Are the bank's standard operating procedures for AML/CFT included in the self-inspection and internal audit items; do operating rules for self-inspection and internal audit specify the circumstances for which enhanced self-inspection and internal audit should be conducted, and whether such rules have been dutifully implemented?	3rd subparagraph, 1st paragraph of Article 6「3. Standard operational procedures for monitoring compliance with AML/CFT regulations and the implementation of the AML/CFT program, which shall be included in the self-inspection and internal audit system, and enhanced if necessary.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
9	Do rules for maintaining AML/CFT related records contain at least: retaining transaction records for at least 5 years; retaining information on verification of customer identity and customer due diligence for at least 5 years after the business relationship is ended, or after the date of the occasional transaction, specifying the role and responsibility of respective units regarding record-keeping, retaining the records of non-bank customer's currency transactions (including records sufficient to permit reconstruction of individual transactions by the bank) above a certain amount in hardcopy	1.6th paragraph of Article 9「A financial institution shall document its operation of ongoing account or transaction monitoring and maintain the records in accordance with Article 12.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended), Financial Supervisory Commission 2. Article 12「A financial institution shall keep records on all business relations and transactions with its customers in hard copy or electronical form and in accordance with the following provisions:1. A financial institution shall maintain all

No.	Examination Item	Legal Basis
	or electronic form (e.g. through the system), retaining name screening records (including list of politically exposed persons (PEP) and sanction list), maintenance and management of suspicious transaction reports, the authority of department in charge of AML/CFT to access customer or transaction data (e.g. making inquiries) and internal control mechanism for swiftly providing customer data to the authority?	necessary records on domestic and international transactions for at least five years or a longer period as otherwise required by law.2. A financial institution shall 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 transactions:(1) All records obtained through CDD measures, such as copies or records of passports, identity cards, driving licenses or other similar official identification documents.(2) Account files (including e-payment accounts and the accounts of electronic stored value card holders) or contract files.(3) Business correspondence, including information on the background and purpose obtained from inquiries to complex, unusual large transactions and the results of any analysis undertaken.3. Transaction records maintained by a financial institution must be sufficient to reconstruct individual transactions so as to provide, if necessary, evidence of criminal activity.4. A financial institution shall ensure that transaction records and CDD information will be available swiftly to the competent authorities when such requests are made with appropriate authority. 」, Regulations Governing Anti-Money

No.	Examination Item	Legal Basis
		Laundering of Financial Institutions (December 14, 2021 Amended) , Financial Supervisory Commission
(B)	Effectiveness of internal controls The following business or sectors (where customers are from) are identified as presenting higher ML/TF risks in NRA(National Risk Assessment) and financial SRA, or for which specific measures must be taken for AML/CFT as stipulated in the laws and regulations set forth by the Financial Supervisory Commission (FSC). However when a bank assesses the risks of customers from the aforementioned sectors, the bank should still give overall consideration to other relevant risk factors. In addition, when evaluating the effectiveness of internal control measures adopted by a bank for transactions involving the following lines of business or customers and for products or services provided, an examiner should also refer to the examination items and results for items under **"Customer Due Diligence", "Ongoing Monitoring and Filing of Suspicious Transaction Report", "Risk Prevention Program and Risk Assessment" and "Organization and Personnel"** of this manual.	
1	**Wire transfer business**	
(1)	Risk factors: This service offers the convenience of transferring large amount of funds	

No.	Examination Item	Legal Basis
	instantly and provides money launderers a channel to quickly transfer funds between accounts or countries. When an inward remittance or cross-border currency transaction involves cash, it possesses higher ML risk. Trade-based cross-border remittances pose relatively high risk of proliferation financing, but due to the lack of substantive transaction documents, and due also to incomplete or untrue information on transaction counterparties, it is not possible to properly monitor and control suspicious transactions and screen names, thus rendering sanctions screening ineffective. When information on the trading counterparty is incomplete, the bank is unable to carry out properly monitoring of suspicious transactions and name screening. The practice of originating bank sending a cover payment message (originating bank sends a MT103 message directly to the bank where the beneficiary has his/her account (beneficiary bank), and in addition, a MT202 message to its cover bank (intermediary bank) for the wire transfer) means the intermediary bank is unable to obtain MT103 or MT202COV message which contains information of the originator and the beneficiary and hence unable to	

No.	Examination Item	Legal Basis
	properly evaluate and manage risks associated with remittance and settlement operations by monitoring suspicious transactions and carrying out name screening. The beneficiary account could be a dummy/nominee account that makes it difficult for the bank to screen the sanction list database and receive a warning.	
(2)	Risk mitigating measures: Obtaining customer due diligence (CDD) information is the most important risk mitigating measure, because adequate and effective internal CDD rules and operating procedures are critical to detecting unusual and suspicious transactions. In addition, an effective system for conducting risk-based monitoring and reporting suspicious transactions is equally important. Regardless whether the system processes the information through an information system or manually, it must be sufficiently effective to detect suspicious trends and suspicious transaction patterns. The bank must periodically conduct a risk-based review of the nature of its customers' trade-based remittances (e.g. the national origin of goods and nationality of transaction counterparties) to determine whether it is consistent with the bank's understanding of the customers.	

No.	Examination Item	Legal Basis
	The bank must periodically conduct a risk-based review of the nature of its customers' trade-based remittances (e.g. the national origin of goods and nationality of transaction counterparties) to determine whether it is consistent with the bank's understanding of the customers. Banks must observe the wire transfer message format and carry out proper name screening and monitoring. Effective monitoring procedures include but are not limited to the following: (1) Establish policies and procedures for account or transaction monitoring using a risk-based approach and use information system to aid in the filtering of MT202COV2 message; (2) an intermediary bank should set up a risk-based approach to identify message with incomplete or meaningless information.	
(3)	Examination items :	
①	Examine whether the bank has established internal AML/CFT rules and operating procedures for its wire transfer business and whether such rules and procedures contain at a minimum internal control measures for mitigating ML/TF risks (e.g. internal control mechanisms for suspicious transaction patterns and for maintaining originator, beneficiary, and transaction information, identity verification	1. 1st to 3rd paragraph of Article 5「A banking business and other financial institutions designated by the FSC shall conduct domestic and cross-border outward and inward wire transfers involving foreign currencies in accordance with the following regulations: 1. Banking business: Conduct wire transfers involving foreign currencies in accordance with the Directions Governing Banking Enterprises for

No.	Examination Item	Legal Basis
	mechanism for customers carrying out cross-border wire transfer, viable subsequent or real-time monitoring to identify inward remittance that lacks originator or beneficiary information, establishing risk-based handling and follow-up procedures, and scope and means of transaction monitoring), and evaluate whether the bank's internal rules and operating procedures are adequate based on the risk factors of wire transfer business (e.g. transaction amount and transaction volume), bank's MIS report on wire transfer business, bank's role in wire transfer (as the originating bank, beneficiary bank or intermediary bank) and size of business.	Operating Foreign Exchange Business. 2. Electronic payment institution: Conduct wire transfers involving foreign currencies in accordance with the Rules Governing the Administration of Electronic Payment Business. 3. Foreign migrant worker remittance company: Conduct wire transfers involving foreign currencies in accordance with the Regulations Governing Small Amount Remittance Services for Foreign Migrant Workers. A banking business and other financial institutions designated by the FSC shall conduct domestic wire transfers involving New Taiwan Dollar (hereinafter referred to as the "NTD") as ordering financial institutions in accordance with the following rules: 1. Provide required and accurate originator information and required beneficiary information by any of the means below: (1) Include information on the originator and the beneficiary accompanying the wire transfer; or (2) Include the account number or a unique transaction reference number which permits the transaction to be traced back to the originator and the beneficiary and make information available within three business days of receiving the

No.	Examination Item	Legal Basis
		request either from the beneficiary financial institution or from appropriate competent authorities. However, Law enforcement authorities should be able to compel immediate production or such information and the banking business shall respond accordingly. 2. Maintain the following required information on the originator and the beneficiary in accordance with Article 12 of the Regulations Governing Anti-Money Laundering of Financial Institutions: (1) The aforementioned originator information shall include: name of the originator, the originator account number where such an account is used to process the transaction (if not available, a unique transaction reference number that permits traceability), and the information by any of the means below: A. National identity number; B. The originator's address; or C. Date and place of birth. (2) The aforementioned beneficiary information shall include: name of the beneficiary and the beneficiary account number (if not available, a unique transaction reference number that permits traceability). A banking business or other financial institutions designated by the FSC that fail to conduct wire transfers in accordance with the two preceding paragraphs are not allowed to

No.	Examination Item	Legal Basis
		engage in wire transfer business.」, 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 (December 14, 2021 Amended) , Financial Supervisory Commission 1st and 2nd subparagraph of 1st paragraph of Point 4「(Outward and inward remittance business) Authorized banks and post offices under the Chunghwa Post Co. Ltd. shall act in accordance with Money Laundering Control Act and relevant rules and in addition, abide by the following provisions when performing domestic and cross-border outward and inward remittance business except a transfer and settlement between a financial institution and another financial institution where both institutions are acting on their own behalf:(1) Outward Remittance Business: i. Documents Required: Operate in accordance with relevant documents filled out by the customer and inspect ID documents or basic registered information. In the case of a company or a firm, query the “company registration inquiry” section or “ business registration inquiry” section in the

No.	Examination Item	Legal Basis
		Commerce Industrial Services Portal of the Ministry of Economic Affairs to confirm the basic registered information of the company or the firm. If the foreign exchange is purchased with the New Taiwan dollar, banking enterprises shall process the settlement in accordance with the "Regulations Governing the Declaration of Foreign Exchange Receipts and Disbursements or Transactions" (hereinafter referred to as “Regulations for Declaration”), and assist the declarant to make a detailed and accurate declaration. ii. Certificates issued: A foreign exchange sale memo shall be issued when the foreign exchange is purchased with the New Taiwan dollar. Other transaction certificates shall be issued when foreign exchange is not purchased with the New Taiwan dollar. The above certificates may be produced in electronic form. iii. Delivering wire transfer: Wire transfer remittance shall include required originator and beneficiary information.(2) Inward Remittance Business: i. Documents required: Operate in accordance with inward remittance notice, foreign currency notes, or foreign currency banknotes, and inspect ID documents or basic registered information. In the case of a company or a firm, query

No.	Examination Item	Legal Basis
		the“ company registration inquiry” section or “business registration inquiry” section in the Commerce Industrial Services Portal of the Ministry of Economic Affairs to confirm the basic registered information of the company or the firm. If the foreign exchange is sold for the New Taiwan dollar, the transaction shall be treated in accordance with the Regulations for Declaration, and assist the declarant to make a detailed and accurate declaration. ii. Certificates issued: A foreign exchange purchase memo shall be issued when the foreign exchange is sold for the New Taiwan dollar. Other transaction certificates shall be issued when foreign exchange is not sold for the New Taiwan dollar. The above certificates may be produced in electronic form. iii. Take following reasonable risk control measures：(i) Take reasonable measures, including post-event monitoring or real-time monitoring where feasible, to identify wire transfers that lack the required originator or beneficiary information.(ii) Implement risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking the required originator or required beneficiary information and the appropriate following-up action where the originator and beneficiary

No.	Examination Item	Legal Basis
		information is insufficient.」, Directions Governing Banking Enterprises for Operating Foreign Exchange Business(November 13 , 2018 Amended), Central Bank
②	Examine whether bank's monitoring of wire transfer business covers at least the following types of transactions and relevant information, and evaluate whether the scope of monitoring is adequate given the size of the bank, types of customers and business complexity: cash-based wire transfer, wire transfer in which the bank being examined acted as the intermediary bank, wire transfer transactions above a certain amount set by the bank originating from (or remitting to) a country or region with higher ML/FT risks.	「Products / Services – Deposit, Withdrawal, or Remittance(12) A customer uses cash that accumulatively reaches a specific amount at a time to make multiple remittances or apply negotiable instruments (e.g. cashier's checks, due-from-bank checks and drafts), negotiable certificates of deposit, traveler's checks, beneficiary certificates, or other securities.(15) The funds remitted from or to high ML/TF risk jurisdictions accumulatively reach a specific amount. The high ML/TF risk jurisdictions described in the Template include but are not limited to the jurisdictions, published by international anti-money laundering organizations and notified by Financial Supervisory Commission, that have serious deficiencies in AML/CFT, and other jurisdictions that fail to comply with or completely comply with the recommendations of such organizations.」, Annex(Red Flags for Suspicious Money Laundering or

No.	Examination Item	Legal Basis
		Terrorism Financing Transactions) of Template of Directions Governing Anti-Money Laundering and Countering the Financing of Terrorism of Banks (April 23, 2019 Amended), The Bankers Association
③	Examine whether the bank has filed a cash transaction report on cash-based wire transfer above a certain amount.	
④	Examine whether there are cases during the determined sampling period where the originator or beneficiary information is missing or meaningless (e.g. customer name is a code) based on the bank's risk assessment result of its wire transfer business, prior examination reports, internal audit report and the electronic files on bank-wide wire transfer transactions taken place during the sampling period (the e-file fields include at least the originator, beneficiary, customer account or the individual serial number of the wire transfer), and if there are cases of missing or meaningless information, understand the reason (to determine whether the bank proceeded with the wire transfer in the absence of adequate information on the originator or the beneficiary), and depending on whether the bank being examined was the originating bank, beneficiary bank or intermediary bank (including	3rd subparagraph of 1st paragraph of Point 4「Intermediary financial institution: i. A financial institution that is an intermediary institution shall retain all the wire transfer originator and beneficiary information accompanying the wire transfer. ii. Where technical limitations prevent the required information accompanying a cross-border wire transfer from importing to the related domestic wire transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution. iii. Items 3 of the preceding Subparagraph shall apply mutatis mutandis.」, Directions Governing Banking Enterprises for Operating Foreign Exchange Business(November 13, 2018 Amended), Central Bank

No.	Examination Item	Legal Basis
	domestic clearing bank) in the related transaction, clarify whether the bank failed to provide originator and beneficiary information as required or failed to follow up on the information of transaction related parties according to its own rules and operating procedures, or failed to retain complete originator and beneficiary information in the wire transfer message in the outgoing remittance message (whether the message format is erroneous).	
⑤	Select a sample of higher risk wire transfer transactions based on the bank's risk assessment result of its wire transfer business, prior examination reports and internal audit report to examine whether the transaction amount, frequency and incoming and outgoing areas of selected transactions are commensurate with the customer's business or occupation (if there is any inconsistency, handle the transaction in accordance with the "**Ongoing Monitoring and Filing of Suspicious Transaction Reports**" section).	
⑥	Select a sample of higher risk wire transfer transactions based on the bank's risk assessment result of its wire transfer business, prior examination reports and internal audit report to determine whether the bank has conducted name screening on its wire transfer	Article 8「Financial institutions shall comply with the following provisions in their watch list filtering programs on customers and connected parties of transactions :1. A financial institution shall establish policies and procedures for watch list filtering, based on a risk-based

No.	Examination Item	Legal Basis
	customers and counterparties based on its established internal rules and operating procedures and saved related records.	approach, to detect, match and filter whether customers, or the senior managerial officers, beneficial owners or connected parties of the customers are individuals, legal persons or organizations sanctioned under the Terrorism Financing Prevention Act or terrorists or terrorist groups identified or investigated by a foreign government or an international organization.2. The policies and procedures for watch list filtering shall include at least matching and filtering logics, implementation procedures and evaluation standards, and shall be documented.3. A financial institution shall document its name and account filtering operations and maintain the records for a time period in accordance with Article 12. 」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended),Financial Supervisory Commission
⑦	Whether the bank performs enhanced due diligence (EDD) on financial transactions involving a specific country or region identified in the letters forwarded by the FSC or relevant law enforcement agencies. In addition, does the bank promptly file a report with the Investigation Bureau, Ministry of Justice on suspicious funds remitted in from	

No.	Examination Item	Legal Basis
	countries or jurisdictions designated by the Financial Action Task Force (FATF) as countries or regions with serious deficiencies in their AML/CFT regime or from other countries or regions that do not or insufficiently comply with the recommendations of international organizations on AML/CFT?	
2	Cross-border correspondent banking and payable-through account	
(1)	Risk factors: When a bank allows a shell bank or a foreign bank that allows a shell bank to use its account to open a correspondent account, it will increase its own ML/TF risks. When a bank allows another bank to open a correspondent account and indirectly handles the transactions of the respondent bank's customers without understanding the customers, it will also expose the bank to ML/TF risks. If the correspondent account opened by the respondent bank involves payable-through account, it means the bank handles directly the transactions of the respondent bank's customers without understanding the customers, and it directly increases the bank's ML/TF risks.	
(2)	Risk mitigating measures: A correspondent bank should perform customer due diligence (CDD) and in addition, gather	1st paragraph of Article 3「Banking businesses and other financial institutions designated by the FSC shall establish specific policies and

No.	Examination Item	Legal Basis
	sufficient publicly available information to understand fully the businesses of the respondent bank and judge its business reputation and management quality, evaluate whether the respondent bank has proper control policies and sufficient implementation effectiveness in AML/CFT. The correspondent bank should obtain the approval of its senior management before establishing a correspondent relationship with another bank, and both the correspondent bank and the respondent bank should have documents established to show each other's AML/CFT responsibility and actions. A correspondent bank (including overseas branches) should establish internal rules and operating procedures to manage ML/TF risks associated with its cross-border correspondent bank account services and closely monitor account related transactions, and detect and report suspicious transactions. Risks associated with cross-border correspondent account have to do with the jurisdiction or country that the respondent bank is in, the attributes of its customers and the products it provides. If the services provided by a correspondent bank to the respondent bank are relatively simple, such as handling cross-border wire transfers on behalf of	procedures for correspondent banking and other similar relationships, including: 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 Anti-Money Laundering and Countering Terrorism Financing (hereinafter referred to as the "AML/CFT") regulations and whether it has been investigated or received regulatory action in connection with money laundering or terrorist financing (hereinafter referred to as the "ML/TF"); 2. Assess whether the respondent bank has adequate and effective AML/CFT controls; 3. Obtain approval from senior management before establishing new correspondent bank relationships; 4. Document the respective AML/CFT responsibilities of each party; 5. Where a correspondent relationship involves in "payable–through accounts", the banking business shall be required to satisfy itself that the respondent bank has performed customer due diligence (hereinafter referred to as the "CDD") measures on its

No.	Examination Item	Legal Basis
	respondent bank's customers, the monitoring of the correspondent account by the correspondent bank should focus on whether the respondent bank carries out name screening and provides information on originator and beneficiary as required.	customers who have direct access to the accounts of the correspondent bank, and is able to provide relevant CDD information upon request to the correspondent bank; 6. The banking business is prohibited from entering into correspondent relationships with shell banks and shall be required to satisfy itself that respondent financial institutions do not permit their accounts to be used by shell banks; 7. For a respondent bank that is unable to provide the aforementioned information upon request, the banking business or other financial institutions designated by the FSC 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; and 8. The aforementioned provisions are also applied to the respondent bank that is a foreign branch or subsidiary of the banking business or financial institutions designated by the FSC.」 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

No.	Examination Item	Legal Basis
		Commission (December 14, 2021 Announced), Financial Supervisory Commission Financial Supervisory Commission Article 11「A bank should establish certain policies and procedures with respect to cross-border correspondent banking or similar business, and the content thereof shall at least include the following: I. Gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to a ML/TF investigation or regulatory action. II. Assess whether the respondent institution has appropriate control policies in place in AML/CFT and the effectiveness of such policies. III. Before establishing cross-border correspondent relationship with the respondent institution, the bank should obtain approval from certain level senior management, determined according to the bank's internal consideration of risk. IV. Document the respective AML/CFT responsibilities of each institution. V. With respect to "payable-through accounts" involved in cross-border correspondent banking, be satisfied

No.	Examination Item	Legal Basis
		that the respondent institution has conducted CDD on the customers having direct access to accounts of the correspondent bank, and that it is able to provide relevant CDD information upon request to the correspondent bank, if necessary. VI. The bank is prohibited from establishing correspondent banking relationship with shell banks or respondent institutions that permit their account to be used by shell banks. VII. For a respondent institution that fails to provide the aforementioned information requested by the bank, the bank may decline to open an account, suspend transactions, report suspicious ML/TF transactions, or terminate the business relationship. VIII. In the case that the respondent institution is the bank’s foreign branch (or subsidiary), aforementioned requirements of this Article also apply.」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures(April 23, 2019 Amended, approved by the Financial Supervisory Commission for recordation), Bankers Association

No.	Examination Item	Legal Basis
(3)	Examination items :	
①	Determine whether the bank offers cross-border correspondent bank account service; Correspondent banking does not include SWIFT Relationship Management Application keys (RMA) in the context of non-customer relationships.	Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and Procedures & "Anti-Money Laundering and Anti-Terrorism Financing Guidelines for the Banking Sector (Template) and Related Regulations: Q&A for financial institutions
②	Examine whether the bank's internal rules and operating procedures regarding cross-border correspondent bank account include at a minimum: the bank may not establish cross-border correspondent relationship with a shell bank or a bank that allows shell banks to use its account, standards and ongoing training for CDD of banks having a cross-border correspondent relationship with the bank, circumstances under which suspicious money laundering transaction report should be filed, internal control procedures for establishing and managing correspondent relationship (including at a minimum CDD, EDD, approval and maintenance procedures for establishing relationship, ongoing monitoring procedure for accounts and transactions), counter measures when the respondent bank is unable to provide CDD information (decline account opening, suspend	

No.	Examination Item	Legal Basis
	transaction, file suspicious transaction report or terminate business relationship), and whether relevant internal rules and operating procedures have been independently reviewed by appropriate personnel to make sure those rules and operating procedures are continuously compliant.	
③	Does the bank retain a copy of the most recent license of the respondent bank or latest data that suffice to show that none of the respondent banks are a shell bank? If the bank has overseas branches, does the bank take reasonable measures to find out whether any of the overseas branches indirectly provides services to a shell bank?	
④	Whether the bank has established risk-based and adequate internal rules and operating procedures for CDD, EDD and monitoring, and relevant CDD procedures (including EDD) may cover the respondent bank's business nature and target markets, purpose of opening an account and anticipated account activities, past correspondence history, publicly available AML records on the respondent bank, requesting the license of overseas respondent bank, whether the jurisdiction or country the respondent bank is in is sanctioned or has high ML/TF risks, obtaining the AML/CFT program of respondent	

No.	Examination Item	Legal Basis
	bank, obtaining the data of customers that have used the payable-through account. In addition, determine whether the internal rules and operating procedures of the correspondent bank have established mechanisms for detection and reporting of correspondent account transactions and for periodically examining whether the transaction status of a respondent bank is consistent with the anticipated account activities and purpose stated at the time of account opening.	
⑤	Select a sample of high risk correspondent accounts based on the bank's risk assessment result of its correspondent banking business, prior examination reports and internal audit report and examine whether the relevant account opening documents or data are complete, whether there is sufficient evidence to corroborate that the account is not used by a shell bank, and for closed correspondent accounts, whether there lacked reasonable cause for establishing a correspondent relationship at the very beginning.	
3	E-banking business It covers all financial products and services offered electronically, including but not limited to ATM services, online account opening, online banking, and phone banking.	
(1)	Risk factors:	

No.	Examination Item	Legal Basis
	Difficulty in confirming the true identity of customer (customer may use another person's real information without authorization to open an account), the customer is not situated in the jurisdiction or country that the bank is located, online transactions occur instantly and can be anonymous, an online banking account can be easily used by a fake company or an unknown third person.	
(2)	Risk mitigating measures: 1. The bank should establish mechanisms to monitor its e-banking business and identify and report suspicious transactions; management information system (MIS) reports that can help detect the transaction activities of high-risk accounts include IP address report and correlated account report (accounts having the same address, telephone number, e-mail address and ID No.). 2. For customers who open an account online, the bank should use effective and reliable method to verify the customer's true identity and establish internal rules to stipulate the circumstances for which a customer may open an account in person only that online account opening is not allowed (e.g. according to prevailing	

No.	Examination Item	Legal Basis
	regulations, a bank can only accept the opening of NTD and foreign currency demand deposit accounts by customers over the Internet or can set other account opening policies based on its own risk management needs). 3. The bank should classify transactions as high risk and low risk based on the impact of the result of executing customer's trading instruction on customer's interests, and design risk-based security measures to protect customer data transmission. 4. The customer identity verification mechanism for online transactions should be commensurate with the AML/CFT risks of the product or service involved. For customers who intend to carry out transactions posing higher ML/TF risk, the bank should adopt multi-factor authentication approach (not relying on a single ID for identification) to mitigate relevant risks.	
(3)	Examination items :	
①	Examine the bank's internal rules and operating procedures for e-banking business and evaluate whether those rules and procedures are adequate in view of the types and risks of e-banking services offered by the bank and whether related internal controls could, to a certain extent, protect the bank from inadvertently	

No.	Examination Item	Legal Basis
	facilitating ML/TF activities. The related internal control system should require name screening of e-banking customers, beneficial owners and trading counterparties and retention of records on ongoing monitoring of customer accounts and transactions in accordance with established internal rules and operating procedures.	
②	Determine whether the bank is capable of effectively identifying and monitoring high risk e-banking accounts or transactions based on the bank's MIS report on its e-banking business and the bank's evaluation of business risk factors (e.g. transaction amount and volume).	
③	Evaluate whether the bank has adequate mechanisms in place for monitoring and reporting suspicious e-banking transactions based on the size, complexity and locations of the bank's e-banking business and the types of transactions its e-banking customers engage in.	
④	Determine whether the bank performs name screening of e-banking customers, beneficial owners and trading counterparties and retention of records on ongoing monitoring of customer accounts and transactions in accordance with established internal rules and operating procedures.	
⑤	Select a sample of high risk e-banking	

No.	Examination Item	Legal Basis
	accounts based on the bank's risk assessment result of its e-banking business, prior examination reports and internal audit report and examine the account opening documents or data (including identity verification data), CDD data over time, and transaction history and compare the anticipated account activities stated in customer data with actual account activities that have taken place to determine whether the customer's account activities are consistent with the stated occupation or business and whether there is any unusual or suspicious transaction.	
⑥	Based on the examination items described above, comment whether the bank's internal rules and operating procedures for e-banking business are adequate and whether the bank's actual operations have been undertaken in accordance with the established internal rules and operating procedures.	
4	E-payment business	
(1)	Risk factors: Given that e-payment business deals with non-face-to-face and possibly anonymous transactions, it makes verifying the identities of buyer and seller and whether the transaction is real difficult. Thus criminals may take advantage of new payment methods to engage in ML/TF activities through fake transactions involving high-price	

No.	Examination Item	Legal Basis
	items.— New payment technology has aided in the quick cross-border transfer and consolidation of illicit funds.	
(2)	Risk mitigating measures: Verify customer identity and do not accept applications to register anonymously or in fictitious names. Carry out ongoing monitoring of accounts and transactions.	
(3)	Examination items :	
①	Examine the bank's internal rules and operating procedures for e-payment business and evaluate whether those rules and procedures are adequate in view of the types and risks of e-payment services offered by the bank and whether related internal controls could, to a certain extent, protect the bank from inadvertently facilitating ML/TF activities. The related internal control system should include user identity verification mechanism, situations under which user's application to register will be declined, conducting name screening on e-payment service users, beneficial owners and trading counterparties and retention of records on ongoing monitoring of user accounts and transactions in accordance with established internal rules and operating procedures.	1st to 3rd subparagraph, 12th subparagraph, 1st paragraph of Article 3「1. A financial institution shall not accept anonymous accounts or accounts in fictitious names for establishing or maintaining business relationship. 2. A financial institution shall undertake CDD measures when: (1) establishing business relations with any customer; (2) carrying out occasional transactions with respect to: A. a single transaction (including domestic remittances) or a certain number (or greater) of electronic stored value card transactions that meet or exceed a certain amount, or multiple clearly related transactions that in sum total meet or exceed a certain amount; or B. a cross-border wire transfer involving NTD 30,000 or more (including the foreign currency equivalent thereof); (3) there is a suspicion of money

No.	Examination Item	Legal Basis
		laundering or terrorist financing; or (4) the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data. 3. The time of establishing business relations with any customer mentioned under Item (1) of the preceding subparagraph is when accepting a customer's registration application in the case of an electronic payment institution, and when accepting a customer's registration of an electronic stored value card in the case of an electronic stored value card issuer. 12. The CDD process for e-payment accounts shall follow relevant provisions in the Regulations Governing Identity Verification Mechanism and Transaction Regulations Governing Identity Verification Mechanism and Transaction Amount Limits of Electronic Payment Processing Institutions, to which the provisions of Subparagraphs (4) ~ (7) hereof do not apply.」 , Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended),Financial Supervisory Commission
②	Determine whether the bank is capable of effectively identifying and monitoring high risk user accounts or transactions based on the bank's MIS report on its e-payment business and	

No.	Examination Item	Legal Basis
	bank's evaluation of business risk factors (e.g. transaction amount, transaction volume, whether cross-border payment is allowed, etc.).	
③	Evaluate whether the bank has adequate mechanisms in place for monitoring and reporting suspicious e-payment activities based on the size and complexity (e.g. whether cross-border payment is allowed) of the bank's e-payment business and the transactions its e-payment customers engage in.	4th and 5th subparagraph, 1st paragraph of Article 9「4. The policies and procedures for account and transaction monitoring of a financial institution shall include at least complete ML/TF monitoring indicators, parameters setting, threshold amounts, alerts and operation procedures of monitoring, the reviewing procedures for monitored cases and reporting standards, and shall be documented. 5. Complete ML/TF monitoring indicators mentioned in the preceding subparagraph shall, based on the business nature of a financial institution, include the suspicious indicators published by the relevant associations and the additional ones developed by the financial institution in reference to its ML/TF risk assessment or daily transaction information. With regard to transfer of funds between e-payment accounts, a financial institution should, when carrying out the monitoring, take into consideration all information received on both accounts to determine whether to file a suspicious ML/TF transaction report.」,Regulations Governing Anti-Money Laundering of Financial
④	Determine whether the bank performs name screening on e-payment customers, beneficial owners and trading counterparties and retention of records on ongoing monitoring of customer accounts and transactions (particularly whether all information on both ends of e-payment transaction (payer and recipient) are taken into consideration) in accordance with established internal rules and operating procedures.	
⑤	Select a sample of high risk e-payment accounts based on the bank's risk assessment result of its e-payment business, prior examination reports and internal audit report and examine the account opening documents or data (including identity verification data), CDD data over time, and transaction history and compare the anticipated	

No.	Examination Item	Legal Basis
	account activities stated in customer data with actual account activities that have taken place to determine whether the customer's account activities are consistent with the stated occupation or business and whether there is any unusual or suspicious transaction.	Institutions (December 14, 2021 Amended),Financial Supervisory Commission
⑥	Based on the examination items described above, comment whether the bank's internal rules and operating procedures for e-payment business are adequate and whether the bank's actual operations have been undertaken in accordance with the established internal rules and operating procedures.	
5	Offshore banking unit (OBU)	
(1)	Risk factors: Given that OBU customers are all offshore companies (particularly private investment firms), it adds to the difficulty of verifying customer identity, CDD and tracking of money flow. Although receipt and payment of actual cash do not necessarily take place when an OBU account makes/receives deposits or wire transfers, the customer can use an OBU account as a payable-through account for laundered money (one stage in the multiple stages of a money laundering crime), thereby posing ML/TF risks.	
(2)	Risk mitigating measures: Verify customer identity, perform	

No.	Examination Item	Legal Basis
	CDD and identify beneficial owner and periodically review and confirm the validity of offshore company's registration. Establish account and transaction monitoring mechanisms to identify, investigate and report suspicious transactions. Suspend the transactions of or suspend or terminate business relationship with terrorists or organizations under economic sanction, or identified or investigated by a foreign government or an international anti-money laundering organization.	
(3)	Examination items :	
①	Examine the bank's internal rules and operating procedures for OBU business and evaluate whether those rules and procedures are adequate in view of the complexity of OBU products, transactions or services offered by the bank and the bank's risk assessment results of its OBU business, and whether related internal controls could, to a certain extent, protect the bank from inadvertently facilitating ML/TF activities. The related internal control system should include customer identity verification mechanism, mechanism for conducting identity verification through intermediaries and entering into a contract with the intermediaries, mechanism for auditing and overseeing	1. Article 11 「Offshore banking branches may rely on the assistance of intermediaries to perform CDD on offshore customers in accordance with these Rules and Money Laundering Control Act or criteria no less stringent than the aforementioned regulations and in compliance with the provisions below. Offshore banking branches shall also report to the FSC of the implementation plan and the list of intermediaries: 1. The act of an intermediary assisting an offshore banking branch in performing CDD conforms to or does not violate the laws and

No.	Examination Item	Legal Basis
	intermediaries' use, handling and control of customer data, acceptable certificate of good standing submitted by OBU customers, and conducting name screening of OBU customers and beneficial owners and retention of records on ongoing monitoring of customer accounts and transactions in accordance with established internal rules and operating procedures.	regulations at where the intermediary is located. 2. The intermediary in the latest audit on its anti-money laundering and combatting terrorism financing operation by the competent authority at where it is located or byan external institution receives a rating of "satisfactory", "no downgrade" or "no material deficiency", or it has taken improvement actions against the deficiency which are accepted as satisfactory by the competent authority or the external institution, or its downgraded rating has been raised. If the intermediary is subsequently downgraded by the competent authority at where it is located or by an external institution or subject to disciplinary action imposed by the competent authority at where it is located due to some material deficiency, the offshore banking branch should suspend the service of the intermediary in performing CDD. 3. An offshore banking branch should sign an agreement with the intermediary it intends to rely on. The agreement should specify the extent of assistance to be rendered by the

No.	Examination Item	Legal Basis
		intermediary in CDD process and proper measures to be taken by the intermediary for confidentiality and maintenance of customer data, and rights and obligations of the parties. The intermediary shall keep the records obtained in performing CDD and provide in a timely manner any document or information obtained in the course of performing CDD upon the request of the offshore banking branch. 4. An offshore banking branch should use a risk-based approach to audit and supervise on a regular and an as-needed basis the intermediary's implementation of CDD process and the intermediary's use, processing and control of customer information; an offshore banking branch may carry out such audit through an appointed externalinstitution. The term "intermediary" referred to in the preceding paragraph means an overseas branch or subsidiary of a domestic bank, the head office or a branch directly under the head office of the branch of a foreign bank in Taiwan, the parent bank ora branch

No.	Examination Item	Legal Basis
		directly under the parent bank of the branch of a foreign bank in Taiwan. The content of "implementationplan" referred to in Paragraph 1 herein shall include at least the scope of CDD performed by anintermediary and intermediary's internal control system for the confidentiality and maintenance of customer data. Offshore banking branches should review the results of CDD performed by intermediaries and bear the ultimate responsibility for the CDD process and data maintenance.」, Rules Governing Offshore Banking Branches(May 22, 2017 modified), Financial Supervisory Commission 3. 2nd paragraph of Article 10「Offshore banking branches shall, before December 31, 2017, re-perform CDD and review the level of risk on existing customers prior to the implementation of these amended Rules promulgated on May 22, 2017. However offshore banking branches shall re-perform CDD immediately in the event of the following situations: 1. The offshore banking branch has doubts about the veracity of

No.	Examination Item	Legal Basis
		customer information, such as there is a suspicion of money laundering in relation to that customer, or there is a material change in the way that the customer's account is operated which is not consistent with the customer's business profile; or 2. It is time for periodic update of customer identityinformation.」, Rules Governing Offshore Banking Branches(May 22, 2017 modified), Financial Supervisory Commission
②	Select a sample of high risk OBU accounts based on the bank's risk assessment result of its OBU business, prior examination reports and internal audit report and examine the account opening documents or data (including identity verification and name screening data) to determine whether the bank's account acceptance documents show any violation of the FSC regulations or inconsistency with the bank's internal rules. In addition, compare the purpose of account and anticipated account activities stated in customer data with actual account activities that have taken place based on CDD data over time and transaction history to determine whether the customer's account activities are consistent with the stated occupation or business, whether there is any unusual or suspicious transaction and whether	Article 12「Offshore banking branches should pay attention to the following when accepting the opening of new accounts: 1. An offshore banking branch shall not refer its onshore customers to agencieswho assist in setting up offshore companies, or induce or assist onshore customers to switch their identity to non-resident status in order to open an account at the offshore banking branch. 2. An offshore banking branch should enhance its understanding of the purpose of a customer opening an account, intended use of the account and planned transaction activities, and the situation, if applicable, where the shareholders, directors or beneficial owners of an offshore legal entity customer include onshore individuals or legal persons, and obtain a customer statement declaring that itdid not

No.	Examination Item	Legal Basis
	the bank has been conducting ongoing monitoring of those sampled accounts.	switch to non-resident status under inducement or for investment in specific products. An offshore banking branch should establish a concrete and viable internal control system for matters specified in the preceding paragraph and implement the system after reporting to the board of directors for approval in the case of a domestic bank or to the head office or regional center for approval in the case of a branch of a foreign bank in Taiwan.」, Rules Governing Offshore Banking Branches(May 22, 2017 modified), Financial Supervisory Commission
6	Insurance business (If the bank has established an "insurance department or division" or sells insurance products through a cooperation or co-selling agreement, it meets the definition of "insurance agent" provided in the Directions Governing Anti-Money Laundering and Countering Terrorism Financing of Insurance Enterprises.)	
(1)	Risk factors: Insurance products can be used in money laundering. For example, insurance products with high policy value reserve (e.g. life insurance and annuity products) can be purchased with black money and then cancelled after a short period of time. When the insurance company returns the money, the connection between the	

No.	Examination Item	Legal Basis
	black money and associated criminal activity becomes blurred. Other signs and patterns of money laundering using insurance products include: when the prospective policyholder cares more about the cancellation clause than return, there may be the possibility of money laundering (for details, see “Patterns or Signs of Suspicious Money Laundering Transactions in Life Insurance”).	
(2)	Risk mitigation measures: The bank should establish internal rules and operating procedures for the following: (1) Identification of high risk customers. (2) Customer due diligence operation (including beneficial owners) and enhanced due diligence (EDD) for high-risk customers. (3) Types of products sold and associated ML/TF risks. (4) Commission system for salespersons. (5) Investigation and reporting of unusual or suspicious money laundering activities. (6) Retention of account and transaction data.	
(3)	Examination details:	
①	Examine the bank’s internal rules and operating procedures for selling insurance products and evaluate whether those rules and procedures	1. 3rd paragraph of Article 5「The AML/CFT program mentioned in Subparagraph 2 of Paragraph 1 hereof shall include the following

No.	Examination Item	Legal Basis
	are adequate in view of the bank's role and risks in the business and whether related internal controls could, to a certain extent, protect the bank from inadvertently facilitating ML/TF activities. The related internal rules and operating procedures should include verification of user identity, situations under which customer's request to establish business relationship or engage in transaction will be declined, obtaining the identity of beneficiary (whether the beneficiary is a legal heir or the designated heir in the will), method and procedure for verifying the identity of beneficiary at the time of payout (whether to include insurance beneficiaries in CDD process. For example, if the bank believes high ML/TF risk is involved when the beneficiary is a legal person or a trustee, the bank should adopt EDD measures to identify and verify the beneficiary's identity before paying the benefit), and setting suspicious money laundering patterns and reporting mechanism.	policies, procedures and controls; the AML/CFT program of insurance agent companies, insurance broker companies and individuals practicing as an insurance agent or broker need not include Items 2 and 3 below 1. Verification of customer identity; 2. Watch list filtering of customers and trading counterparties; 3. Ongoing monitoring of transactions; 4. Record keeping; 5. Reporting of currency transactions above a certain amount; 6. Reporting of suspicious money laundering or terrorist financing transactions. 7. Appointment of a compliance officer at the management level to take charge of AML/CFT compliance matters; 8. Employee screening and hiring procedure; 9. Ongoing employee training program; 10. An independent audit function to test the effectiveness of AML/CFT system; and
②	Evaluate whether the bank is capable of effectively identifying the sales of insurance products with high policy reserve value, and whether the bank's investigation and reporting of suspicious transactions are commensurate with the size and complexity of this type of business	11. Other matters required by the AML/CFT regulations and the competent authorities」, Regulations Governing Implementation of Internal Control and Audit System for Anti-Money Laundering and Countering Terrorism Financing of Insurance

No.	Examination Item	Legal Basis
	and ML/TF risks presented by the customers based on the role of the bank (including post offices) in the business (e.g. whether the bank handles underwriting and claims on behalf of the insurance company), and customer and transaction information obtained by the bank therefrom, the bank's MIS report on the business and the bank's evaluation of business risk factors.	Companies, Post Offices Engaging in Simple Life Insurance Business and Other Financial Institutions Designated by the Financial Supervisory Commission(November 9, 2018 Amended), Financial Supervisory Commission 2.7th subparagraph of Article 3「(4) Except for situations provided for in the proviso of Subparagraph 3, Paragraph 1of Article 6 herein, a financial institution is not subject to the requirements of identifying and verifying the identity of beneficial owner(s) of a customer set out under Item (3)of Subparagraph 4hereof when the customer purchases property insurance, accident insurance, health insurance or an insurance product that does not require policy value reserve.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended),Financial Supervisory Commission 3.Article 11「Insurance agent companies that solicit insurance policies on behalf of insurance companies in accordance with Article 8 of the Insurance Act and insurance broker companies that negotiates an insurance policy or provides related services on the basis of the interests of the insured in accordance with Article 9 of the

No.	Examination Item	Legal Basis
		Insurance Act may be exempted from the provisions of ongoing customer due diligence provided in Article 5 and Article 6 herein, the policies and procedures for watch listing filtering provided in Article 8 herein, ongoing monitoring of transactions provided in Article 9 herein and provisions on PEPs in the preceding Article. However if an insurance agent company undertakes underwriting and claim settlement business on behalf of an insurance company, the insurance agent company shall comply with the provisions of these Regulations on insurance company with respect to its policies, procedures and controls for its agency business.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended), Financial Supervisory Commission 4.3rd subparagraph of Article 4「3. Where any person acts on behalf of a customer to open an account, register a stored value card, register an e-payment account, apply for insurance, file an insurance claim, request a change of insurance contract or conduct a transaction, it is difficult to check and verify the fact of authorization and identity-related information;」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended),

No.	Examination Item	Legal Basis
		Financial Supervisory Commission 5.3rd subparagraph of Article 6「An insurance enterprise should consider the beneficiary of a life insurance policy as a relevant risk factor in determining whether to apply enhanced CDD measures. If the insurance enterprise determines that a beneficiary who is a legal person or a trustee presents a higher risk, the enhanced CDD measures should include reasonable measures to identify and verify the identity of the actual beneficiary before making benefit payout.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended), Financial Supervisory Commission 6. 8th subparagraph of Article 3「8. An insurance enterprise shall adopt the following measures when the beneficiary(ies) on a life insurance policy, investment-linked insurance policy or annuity insurance policy have been identified or designated: (1)Obtaining the name and identification document number or registration (incorporation) date of the designated beneficiary; and (2)For beneficiary(ies) that are designated by contract characteristics or by other means, obtaining sufficient information concerning the beneficiary to satisfy the insurance enterprise

No.	Examination Item	Legal Basis
		that it will be able to establish the identity of the beneficiary at the time of the payout.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended), Financial Supervisory Commission 7.3rd paragraph of Article 10「Insurance companies and post offices engaging in simple life insurance business should take reasonable measures to identify and verify whether the beneficiary of a life insurance policy, investment-linked insurance policy or annuity insurance policy and the beneficial owner of the beneficiary are PEPs referred to in the preceding paragraph before paying out benefit or cash surrender value. In case high risk circumstances are discovered, an insurance enterprise should, prior to paying out policy proceeds to PEPs, inform senior management, conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious ML/TF transaction report.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended), Financial Supervisory Commission 8.10th subparagraph of Article 3「Where a financial institution is unable to complete the required CDD process on a customer, it

No.	Examination Item	Legal Basis
		should consider filing a suspicious transaction report on money laundering or terrorist financing (STR)in relation to the customer.」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended), Financial Supervisory Commission
③	Select a sample of large life insurance, investment-linked insurance and annuity policies where the underwriting or claim or contract change is handled by an agent of the policyholder to examine whether the bank has verified the fact of agency and the agent's identity and saved related data; in addition, select a sample of large life insurance, investment-linked insurance and annuity policies to examine whether the bank has verified the identity of insurance beneficiary and saved complete record.	
④	For banks that handle payment or claims for the insurance company, select a sample of large life insurance, investment-linked insurance and annuity policies with high ML/TF risk beneficiaries to examine whether the bank has identified and verified the beneficial owners of the beneficiaries and save related data; if the beneficiary or beneficial owner of an insurance policy is a politically exposed person	

No.	Examination Item	Legal Basis
	(PEP) posing high ML/TF risk or the bank is unable to identify or verify the beneficiary or beneficial owner, does the bank adopt measures to evaluate and report suspicious transactions and save related investigation and judgment records?	
7	International trade finance (not limited to traditional import/export documentary bill business)	
(1)	Risk factors: The involvement of multiple parties in the transaction makes it difficult to the bank to conduct CDD, and as trade finance involves a considerable number of documents, the problem of a customer forging documents for ML/TF purpose may arise. The bank should stay alert of higher risk goods that the trade finance is for and should try its best to verify the reasonableness of the price of the goods to prevent the proceeds of crime from being transferred across borders, for example, using false invoice that jacks up the prices of imported goods to transfer proceeds of crime across the border. If the applicant for issue of documentary bill is an offshore nominee or shell corporation, it might cover the identity of the real applicant or beneficiary, thereby increasing ML/TF risk.	
(2)	Risk mitigating measures: The bank should establish a sound CDD process to understand fully the	

No.	Examination Item	Legal Basis
	real business of a customer and the customer's business place, and the bank needs to adopt different levels of CDD measures in view of the role it plays in trade finance. For example, a bank that issues letter of credit needs to perform adequate CDD before granting a line of credit to a customer, including information on the applicant and the beneficiary, sources of funds, nature of business, etc. If the business place of the customer is located in a jurisdiction posing higher ML/TF risk, the bank may need to perform additional background investigation, and when undertaking international trade finance, the bank should understand fully the contents of documents. In addition, the bank can refer to guidance and best practices for banks published by Wolfsberg Group, FATF and APG for risk mitigating measures. The bank should watch if there is any irregularity or signs of money laundering when undertaking international trade finance. If there is any irregularity, it does not necessary mean a suspicious transaction report (STR) should be filed. But the bank needs to conduct investigation and verification to determine whether suspicious activity is involved. The bank should establish internal rules and operating procedure (including: how to examine the accuracy of documents presented by the	

No.	Examination Item	Legal Basis
	customers, telltale signs of money laundering, name screening of customers and beneficial owners, internal procedure for reporting suspicious money laundering transactions, and retention of transaction records), and based on which, make judgment when handling actual transactions and making necessary reporting. Red flags of money laundering include but are not limited to the following: (1) The delivered goods or destination is inconsistent with the industry or line of business the customer is in or is unrelated to the nature of customer's business operation, or if the delivered goods is inconsistent with the description in the bill of lading and payment order or invoice, such as the quantity or type of imported/exported goods not matching. (2) The goods are shipped to or from a high ML/TF country or jurisdiction or the customer comes from high ML/TF country or jurisdiction. (3) The customer is involved in suspicious or high ML/TF risk activity, including importing or exporting goods that are subject to embargo or import/export restrictions (e.g. equipment for military organizations of foreign	

No.	Examination Item	Legal Basis
	governments, weapons, chemicals, metals or other natural resources). (4) The pricing of product and service or the value declared in invoice is obviously inconsistent with the fair market value (underpricing or overpricing). (5) The transaction structure appears to be unnecessarily complex and designed to obscure the true nature of the transaction or source of funds. (6) The method of payment does not match the risk characteristics of the trade. For example, prepayment is made to a new supplier located in a high ML/TF risk country or jurisdiction or the customer requests payment of proceeds to an unrelated third party. (7) The letters of credit used in trade are frequently amended or significantly amended, extended or location of payment is changed without reasonable justification. (8) Using letter of credit, bill discount or other means that is not trade based in offshore financing. (9) The type of goods shipped is susceptible to being used in money laundering or terrorist financing, such as high value goods but available in small quantity (e.g. diamonds and artworks).	

No.	Examination Item	Legal Basis
(3)	Examination items :	
①	Examine and evaluate whether the bank includes relevant controls into internal rules and operating procedures based on risks and whether relevant rules can reasonably protect the bank from ML/TF risks.	
②	Evaluate whether the information obtained by the bank in CDD is adequate.	
③	Evaluate whether the bank is capable of effectively identifying and monitoring suspicious or unusual higher risk international trade finance transactions based on relevant MIS report of the bank and its evaluation of business risk factors.	
④	Evaluate whether the bank's monitoring of international trade finance transactions is adequate and commensurate with its size, complexity, geographic location or customer portfolio.	
⑤	When necessary, the examiner can conduct verification according to the following procedure: i Select samples based on the bank's risk assessment result of its international trade finance transactions, internal audit report and prior examination reports to examine whether the information obtained by the bank in CDD is commensurate with the customer risk and to identity whether there is any unusual or suspicious	

No.	Examination Item	Legal Basis
	transaction. ii Determine whether the bank conducts name screening of transaction related customers and beneficial owners, monitors suspicious transactions, and retains related CDD data.	
8	Corporate organization (Company limited by shares or Limited Company that are Non-Public Companies) and Legal trust	
(1)	Risk factors: A corporate organization and legal trust have the advantage of concealing the true owners of assets that may be connected to criminal activities. Moreover, verifying the beneficial owners of a corporate organization and legal trust is more difficult. Because of the lack of ownership transparency and because not all companies are required to disclose or retain their financial information and corporate operations cover a wide range of businesses, corporate customers, including offshore corporate customers pose higher ML/TF risk to banks. The following are suspicious activity indicators related to companies and legal trust: (1) Lacking sufficient information to positively identify beneficial owners or beneficiaries of accounts or other banking activities (companies and legal	

No.	Examination Item	Legal Basis
	trust). (2) Payments to or from the company have no stated reason, or the reason or relevant documentation is inadequate. (3) Goods or services that the payments are to or from the customer do not match profile of company provided by the foreign remitting bank or the information on the customer's stated business items, or explanation given by the originating bank or beneficiary's bank on the purpose of transaction is inconsistent with observed funds transfer activity. (4) Transacting businesses share the same address, provide only a registered agent's address, or have other address inconsistencies. (5) Many funds transfers are sent in large, round dollar. (6) Unusually large number and variety of beneficiaries are receiving funds transfers from one company. (7) Complex and high-value payments or transfers between companies or legal trust with no apparent legitimate business purpose.	
(2)	Risk mitigating measures: The bank should establish internal rules and operating procedures for identifying the account risks of the above mentioned corporate	

No.	Examination Item	Legal Basis
	customers. The bank should assess the ML/TF risks of the above mentioned corporate customers and carry out ongoing account and transaction monitoring on the basis of risk.	
(3)	Examination items :	
①	Evaluate whether the bank's internal rules can reasonably protect the bank from ML/TF risk based on the ML/TF risk associated with the transactions between the bank and the above mentioned corporate customers.	
②	Confirm the additional CDD measures taken by the bank for the above mentioned corporate customers and evaluate whether those additional measures are commensurate with customer risk or have any deficiency.	
③	Evaluate whether the bank can effectively identify and monitor high risk accounts based on the bank's MIS report and its risk assessment result of its corporate customers.	
④	Evaluate whether the bank system for monitoring the above mentioned corporate customers and reporting suspicious money laundering transactions (identification by system or manually or both) is adequate for the dealings between the bank and its corporate customers.	
⑤	Select a sample of high risk customers (e.g. customers from high risk country or jurisdiction, accounts with large amounts of cash deposited or withdrawn frequently, the	

No.	Examination Item	Legal Basis
	customer has issued bearer shares, the customer has multiple business relationships with the bank, the customer is controlled by a private company or has conducted a transaction for which the bank has filed a suspicious transaction report) based on the bank's risk assessment result of its corporate customers, internal audit report or prior examination reports to examine whether the bank has conducted adequate CDD for the sampled customers, whether the CDD data are complete, and whether the customer account has any unusual or suspicious activity based on the stated purpose of the account and other information. Particular attention should be given to customer transactions that involve higher risk product or service offered by the bank to evaluate the adequacy and effectiveness of the bank's internal rules and internal controls.	
9	Politically exposed persons (PEPs) (including those who are no longer entrusted with a prominent public function but are still with influence)	1. 3rd paragraph of Article 7 「Financial institutions and designated nonfinancial businesses or professions shall apply a risk-based approach to conduct enhanced customer due diligence measures for a customer or beneficial owner who is a politically exposed person currently or previously entrusted with a prominent public function by the domestic or a foreign

No.	Examination Item	Legal Basis
		government or an international organization, as well as his or her family members and close associates」,Money laundering Act(November 7, 2018 Amended), Ministry of Justice 2. Article 5「Financial institutions and designated nonfinancial businesses or professions shall still adopt a risk-based approach to the politically exposed persons listed in Article 2 to Article 4 who are no longer entrusted with a prominent public function, to assess their influence and identify whether Paragraph 3 of Article 7 of the Act still applies to them.」, Standards for Determining the Scope of Politically Exposed Persons Entrusted with Prominent Public Function, Their Family Members and Close Associates(October 16, 2018 Amended), Ministry of Justice
(1)	Risk factors: In cases over the past few years, PEPs have used banks as conduits for their illegal activities, including corruption, bribery, and money laundering. Not all politically exposed persons (PEPs) pose the same risk. Risk factors associated with PEPs include the country or jurisdiction the PEP is from (e.g. whether the source of funds or the customer is from a high risk country or jurisdiction, whether	Q & A on「Standards for Determining the Scope of Politically Exposed Persons Entrusted with Prominent Public Function, Their Family Members and Close Associates」

No.	Examination Item	Legal Basis
	the customer is a domestic PEP, etc.), customer's line of business (e.g. when the customer is a legal person, CDD should be performed on beneficial owner, whether the line of business the customer is in involves primarily cash transactions, etc.), social status and political influence(for those who are no longer entrusted with a prominent public function, the following factors shall be considered:1. The seniority of the position that the person held as a politically exposed person.2. Whether the person's previous and current function are linked in any way). In addition, considerations should be given to PEP's purpose of the account, anticipated account activities and transaction amounts, bank products or services needed, risk level or complexity of planned business relationships with bank, and bank's own vulnerabilities in risk assessment and CDD to determine whether a customer is a high-risk PEP.	
(2)	Risk mitigating measures: The bank should establish rules and operating procedures for risk-based CDD and ongoing monitoring of PEP accounts and transactions. In particular, risk-based account opening rules and operating procedures should be established for large-sum accounts opened by PEPs or PEPs who plan to undertake	1. Article 10「When conducting CDD measures, a financial institution should use self-established database or information obtained from external sources to determine whether a customer and its beneficial owner or senior managerial officer is a person who is currently or has been

No.	Examination Item	Legal Basis
	higher risk transactions. The bank should take the opportunity of a customer applying to open an account to obtain all customer-related information. For high risk PEPs or PEPs with whom the business relationship is deemed high risk, CDD measures the bank should adopt include the CDD measures set out in Article 3 of the Regulations Governing Anti-Money Laundering of Financial Institutions, and additionally, at a minimum the following enhanced measures: (1) Obtaining the approval of senior management before establishing or entering a new business relationship; (2) Taking reasonable measures to understand the sources of wealth and the source of funds of the customer; the source of funds means the actual source from which the funds are derived; (3) Conducting enhanced ongoing monitoring of business relationship; and (4) Confirming whether any family members or close associates of the PEP has controlling ownership interest of the account or can benefit from the account. The bank should ensure that its customer information is readily updated, its employees receive training regularly, and that it uses Internet and electronic media resources (e.g. property filing	entrusted with a prominent public function by a foreign government or an international organization (referred to as politically exposed persons (PEPs) hereunder): 1. For a customer or the beneficial owner thereof determined to be a current PEP of a foreign government, a financial institution shall treat the customer directly as a high-risk customer, and adopt enhanced CDD measures under Subparagraph 1, Paragraph 1 of Article 6. 2. For a customer or the beneficial owner thereof determined to be a current PEP of the domestic government or an international organization, a financial institution shall assess the PEP's risks when establishing business relationship with the PEP and conduct annual review thereafter. In case of higher risk business relationship with such customers, the financial institution shall adopt enhanced CDD measures under Subparagraph 1, Paragraph 1 of Article 6. 3. For a senior managerial officer of a customer determined to be a current PEP of the domestic government, a foreign government or an international

No.	Examination Item	Legal Basis
	system, customer's declaration (however customer's declaration does not relieve the bank of its responsibility), information sharing within the group, commercial database or TDCC (Taiwan Depository & Clearing Corporation) database). However the bank's use of database is not a substitute for its CDD process, for database has its limitations.	organization, a financial institution shall determine whether to apply the enhanced CDD measures under Subparagraph 1, Paragraph 1 of Article 6 considering the officer's influence on the customer. 4. For a PEP who is no longer entrusted with a prominent public function by the domestic government, a foreign government or an international organization, a financial institution shall assess the influence that the individual could still exercise by considering relevant risk factors and determine whether to apply the provisions of the preceding three subparagraphs based on the RBA. 5. The preceding four subparagraphs apply to family members and close associates of PEPs. The scope of family members and close associates mentioned above will be determined by the regulations stipulated in the latter part of Paragraph 4, Article 7 of the Act. Provisions of the preceding paragraph do not apply when the beneficial owner or senior managerial officer of a customer specified under sub-items (A) ~ (C) and (H) of Item (3), Subparagraph 7 of Article 3 is a PEP. Insurance companies and post

No.	Examination Item	Legal Basis
		offices engaging in simple life insurance business should take reasonable measures to identify and verify whether the beneficiary and its beneficial owner of a life insurance policy, investment-related insurance policy or annuity insurance policy are PEPs referred to in the preceding paragraph before paying out benefit or cash surrender value. When high risk circumstances are discovered, an insurance enterprise should, prior to paying out policy proceeds to PEPs, inform senior management, conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious ML/TF transaction report.」, Regulations Governing Anti-Money Laundering of Financial Institutions (November 14, 2018 Amended),Financial Supervisory Commission 2. Q&A on "Standards for Determining the Scope of Politically Exposed Persons Entrusted with Prominent Public Function, Their Family Members and Close Associates", June 28 ,2017, Ministry of Justice 3. Article 6「A financial institution shall determine the extent of applying CDD and ongoing due

No.	Examination Item	Legal Basis
		diligence measures under Subparagraph 4 of Article 3 and the preceding article based on a risk-based approach (RBA): 1. For higher risk circumstances, a financial institution shall perform enhanced CDD or ongoing due diligence measures, including adopting at least the following additional enhanced measures: (1) Obtaining the approval of senior management before establishing or entering a new business relationship; (2) Taking reasonable measures to understand the sources of wealth and the source of funds of the customer. The aforementioned source of funds refers to the substantial source from which the funds generate; and (3) Conducting enhanced ongoing monitoring of the business relationship. 2. For customers from high ML/TF risk countries or regions, a financial institution shall conduct enhanced CDD measures commensurate with the risks identified. 」, Regulations Governing Anti-Money Laundering of Financial Institutions (November 14, 2018 Amended),Financial Supervisory Commission
(3)	Examination items :	
①	Whether the bank determines the	

No.	Examination Item	Legal Basis
	risk level of PEP customers and their family members and close associates as required or on the basis of risk; whether the bank's risk assessment methods and rules and operating procedures for risk-based CDD, account opening and ongoing monitoring of accounts and transactions are adequate.	
②	Evaluate whether the bank's PEP risk assessment methods, MIS system and transaction monitoring reports can effectively identify and monitor business relationships with PEP (particularly high-risk PEPs or PEPs with whom the business relationship is deemed high risk) and suspicious transactions.	
③	Determine whether the bank's CDD, account opening procedure and ongoing monitoring of accounts and transactions of high-risk PEPs comply with the local regulations and the bank's own rules based on the bank's risk assessment result of its PEP customers, prior examination reports, and internal audit report.	
10	Professional service providers (including CPAs, lawyers, and real estate brokers)	
(1)	Risk factors: Professionals accept engagements from many different types of customers, and the services they provide are intricate (e.g. tax planning, corporate establishments, brokered trading of securities or real	

No.	Examination Item	Legal Basis
	estate, etc.). In the course of such activities, there are opportunities to help customers sign fake contracts or documents.	
(2)	Risk mitigation measures: In establishing and maintaining business relationships with a customer, the bank must thoroughly assess its risks and monitor for suspicious or irregular transactions or activities. During the account opening process, the bank must understand how the customer expects to use the account, including the expected transaction amounts, the related products and/or services, the geographic locations of counterparties, and whether transactions involve the conduct of high-transactions (e.g. real estate transactions, corporate establishments, asset custodian services) by high-risk third parties (i.e. customers who provide professional services).	
(3)	Examination items	
①	Based on the relationships between the bank and professional service providers, and the associated risks, assess the adequacy of the examined institution's policies, procedures, and processes.	
②	Check the examined institution's internal risk rating factors and determine whether the bank is capable of effectively identifying and monitoring its relationships with	

No.	Examination Item	Legal Basis
	professional service providers, and the associated risks.	
③	Conduct sampling checks on higher-risk professional service providers, and determine whether the examined institution's ongoing monitoring measures are sufficient to identify possible money laundering transactions.	
11	Jewelry shops	
(1)	Risk factors: The products sold by jewelry shops feature high unit prices, high value, small size, and easy portability, and attract little attention. Moreover, the quick speed of cash transactions makes it difficult for jewelry shops to understand customers, so they are easily used for money laundering.	
(2)	Risk mitigation measures The bank must adopt policies, procedures, and processes for identifying high-risk relationships. During the account opening process and throughout the course of such relationships, the bank must periodically carry out due diligence to assess money laundering risk, and it must include such relationships in its monitoring of suspicious activity. During the account opening process, the bank must understand the customer's business operations and how the customer intends to use the account, including the expected transaction volume, the related products and/or services, and the	

No.	Examination Item	Legal Basis
	geographic locations of counterparties. The bank must direct its resources toward accounts that pose the greatest ML/TF risk. The following factors can be used to identify risks: purpose of account; amount, frequency, and nature of cash transactions; customer's history (including length of the business relationship, and whether STRs or CTRs have been filed against it); the products sold in the customer's main line of business (e.g. uniformly priced diamonds, gold and platinum bars, loose diamonds, and other items that are highly liquid, have a large market, and are likely to sell quickly; jewelry made of gold and precious stones, which are more difficult to sell and tend to sell at a relatively large discount); the geographic area involved and the country (or countries) where the customer does business; and how cooperative the customer was in providing information.	
(3)	Examination items	
①	Based on the relationships between the bank and jewelry shops, and the associated risks, assess the adequacy of the examined bank's policies, procedures, and processes.	
②	Check the examined institution's internal risk rating factors and determine whether the bank is capable of effectively identifying and	

No.	Examination Item	Legal Basis
	monitoring its relationships with jewelry shops, and the associated risks.	
③	Conduct samplings checks on higher-risk jewelry shops, consider the reasonableness of their cash transactions, and determine whether the examined institution's ongoing monitoring measures are sufficient to identify possible money laundering transactions.	
13	Non-profit organizations (civic organizations, national religious organizations, and social welfare or charity organizations)	
(1)	Risk factors Non-profit organizations can be used to raise funding for charity or religious organizations, therefore the internal and external funds flows of non-profit organizations can be very complex, and the anonymity of donors means that non-profit organizations can be abused for illicit purposes. Accordingly, they have relatively pronounced ML/TF vulnerabilities.	
(2)	Risk mitigation measures: To assess the risks of a customer that is a non-profit organization, the bank must conduct thorough due diligence on the organization, in addition to all necessary due diligence on the customer, and in its due diligence on the organization the bank must also emphasize other aspects, such as: the organization's stated activities	

No.	Examination Item	Legal Basis
	and goals; the geographic location of its service area (including the head office and all operating areas); organizational structure; the place of origin of the donors and volunteers; contribution standards (including information on beneficial owners); records retention requirements; relationships with other non-profit organizations and government organizations; and internal controls and audits. Possibly higher-risk non-profit organizations include those that have international operations or provide international services, and those that conduct unusual or suspicious activities or lack proper documentation. Enhanced due diligence measures for these high-risk organizations could include the following: assessing the organization's representatives or administrators; obtaining and reviewing financial statements; checking sources and utilization of funds; and assessing non-profit organizations' larger donors.	
(3)	Examination items:	
①	Check the examined institution's internal risk rating factors and determine whether the bank is capable of effectively identifying and monitoring its relationships with non-profit organizations, and the associated risks.	
②	From a review of MIS and internal	

No.	Examination Item	Legal Basis
	risk rating factors, determine whether the bank effectively identifies and monitors the accounts of high-risk government organizations.	
③	Determine whether the bank's system for monitoring the accounts of non-profit organizations for suspicious activities, and for reporting suspicious activities, is adequate given the bank's size, complexity, location, and types of customer relationships.	
13	Virtual Currency Exchanger	
(1)	Risk factors Virtual currency systems can be traded on the Internet, are generally characterised by non-face-to-face customer relationships, and may permit anonymous funding. They may also permit anonymous transfers, if sender and recipient are not adequately identified. Virtual currency systems can be used to make cross-border payments and funds transfers.	
(2)	Risk mitigation measures: Risk rated Virtual Currency Exchanges high and enhanced measures taken accordingly.	
(3)	Examination Items	The FSC’s letter dated July 27,2018 to all supervised banks and credit unions The FSC’s letter dated October 4,2018 to all supervised banks and credit unions
①	Whether the inspected institution understands the purpose of the customer's business relationship and whether the customer is a virtual currency exchanger.	
②	The inspected institution should	

No.	Examination Item	Legal Basis
	confirm the virtual currency exchanger's identity and that the virtual currency users registered to the exchanger with their real names.	
③	Whether the inspected institution list virtual currency platform operators as high-risk customers, and take enhanced customer identification (EDD) measures, and add relevant red flags to monitor the exchanger and its users.	
E	**Organization and Personnel**	
(A)	To successfully implement its AML/CFT program, is the bank prudent in employee hiring and is the training arranged for employees adequate?	1st subparagraph of Article 9「A banking business and other financial institutions designated by the FSC shall establish screening procedures to ensure high standards when hiring employees, including examining whether the prospective employee has character integrity and the professional knowledge required to perform its duty.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
1	Whether the bank has internal rules and operating procedures in place for employee screening and hiring; the screening and hiring (including change of position) criteria should include at least examining whether the prospective employee has	

No.	Examination Item	Legal Basis
	character integrity and the professional knowledge required to perform his/her duty and whether the examination operation has workpapers saved. The examiner should focus on the screening and hiring criteria established by the bank. With regard to passive criteria, does the bank confirm that the background of an employee will not impede his/her duties in AML/CFT operation, and the bank can establish different screening and hiring criteria for employees at different positions based on the ML/TF risk associated with their duties. Those criteria include but are not limited to: whether the employee comes from a high-risk or sanctioned jurisdiction or has a criminal record on ML/TF related offense. With regard to positive criteria, does the bank determine whether the employee has adequate professional knowledge required to perform his/her AML/CFT duty.	
2	When an employee has any of the following situations, the bank should make sampling check the works handled by the employee, and if necessary, ask its audit unit to assist in investigation: ① The employee exhibits a lavish lifestyle that cannot be supported by his or her salary. ②The employee is reluctant to take a scheduled vacation without a	5th paragraph of Article 18，Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing Policies and procedures, Banker's Association (Approved by FSC on 2019.04.23)

No.	Examination Item	Legal Basis
	reason. ③ The employee cannot give a reasonable explanation to the large amount inflow or outflow in his/her account.	
3	Whether the bank sets the hours of AML/CFT training its directors, supervisors, president, legal compliance personnel, internal auditors and business personnel (except chief AML/CFT compliance officer, AML/CFT compliance unit personnel and AML/CFT supervisor of domestic business units) should receive every year and makes the training mandatory.	1. 5th paragraph of Article 9「A banking business and other financial institutions designated by the FSC shall annually arrange appropriate hours and contents of orientation and on-the-job training on AML/CFT for its directors (council members), supervisors, president, legal compliance personnel, internal auditors, and business personnel in view of the nature of its business, to familiarize them with their AML/CFT duties and equip them with the professional knowhow to perform their duties.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Amended), Financial Supervisory Commission 2.7th paragraph of Article 18「A bank may take following measures to conduct orientations and trainings: I. Orientations: a bank should arrange orientations to include at least certain-hour training classes on AML/CFT regulatory requirements and legal
4	Whether the training covers laws and regulations set forth by the competent authorities, bank's relevant rules and operating procedures (including the responsibilities of relevant personnel with regard to their AML/CFT duties), internal violation cases and disciplinary actions imposed by competent authorities against the bank, and regulations newly promulgated by competent authorities and revisions of internal rules and operating procedures in response to regulatory changes.	

No.	Examination Item	Legal Basis
		responsibilities of employees of financial services industry to allow new employees to understand relevant regulatory requirements and responsibilities. II. Training: (I) Initial trainings on regulatory requirements: after Money Laundering Control Act and Counter-Terrorism Financing Act enter into force or get amended, the bank should conduct trainings on such regulatory requirements for employees within a shortest period to introduce Money Laundering Control Act, Counter-Terrorism Financing Act, and relevant regulatory requirements, and explain the bank's relevant measures in response to those changes. AML/CFT responsible unit should be responsible for planning such trainings and having employee training unit implement the trainings. (II) Regular training: 1. Each year employee training unit should periodically conduct relevant trainings for employees to learn, in order to strengthen the judgment of employees, implement AML/CFT functions, and prevent employees from non-compliance. Such trainings may be arranged into other professional trainings to include appropriate relevant

No.	Examination Item	Legal Basis
		classes. 2. The trainings may be instructed by employees trained by the bank. In addition, the bank may invite scholars or experts as instructors if necessary. 3. To allow employees to sufficiently understand the characteristics and types of ML/TF in order to facilitate the identification of "suspicious ML/TF transactions", the trainings should be supplemented by real cases in addition to the introduction of relevant regulatory requirements. 4. AML/CFT responsible unit should periodically understand an employee's attendance in trainings. For an employee who never attends, AML/CFT responsible unit should urge the employee to attend relevant trainings if necessary. 5. In addition to internal trainings, the bank may select employees to attend trainings provided by external training institutions. III. Lectures for specific topics: in order to enhance employees' understanding of AML/CFT regulatory requirements, the bank may conduct lecturers for specific topics and invite scholars or experts to visit the bank as lecturers.」, Model Guidelines for Banks' Anti-Money Laundering and Counter Terrorism Financing

No.	Examination Item	Legal Basis
		Policies and procedures, Banker's Association (Approved by FSC on 2019.04.23)
5	Whether the bank arranges different training programs for employees facing different ML/TF risks (e.g. front desk staff and back office staff face different ML/TF risks, and the risks faced by trust department and deposit/wire transfer department differ).	
6	Whether any bank employee has misconduct that violates AML/CFT regulations.	2nd paragraph of Article 17 「Employed personnel prescribed in paragraphs 1 to 3 of Article 5, who are not public officials, and who disclose or deliver documents, pictures, information or objects relating to reported transactions suspected of violating provisions under Articles 14 and 15, or to suspected offences described in Articles 14 and 15, will f shall be sentenced to imprisonment of not more than two year, a detention, or a fine of not more than NT$500,000.」, Money Laundering Control Act (November 7, 2018 Amended), Ministry of Justice
(B)	Dedicated compliance unit and chief AML/CFT compliance officer:	
1	Whether the bank has set up an independent, dedicated AML/CFT compliance unit under the president, or under the legal compliance unit or risk management unit of the head office and whether the AML/CFT	1. 1st subparagraph, 1st paragraph of Article 7 「A banking business and other financial institutions designated by the FSC shall be staffed with adequate number of AML/CFT personnel and

No.	Examination Item	Legal Basis
	compliance unit handles businesses other than AML/CFT.	resources appropriate to the size and risks of its business. The
2	Whether the bank has appointed a senior officer to act as the chief AML/CFT compliance officer and whether the officer has sufficient authority to coordinate the implementation of AML/CFT program by units throughout the bank. The examiner should check the relevant delegation of authority table to confirm the actual authority of the officer and understand whether it has been so implemented in actual operation.	board of directors (council) of the banking business and other financial institutions designated by the FSC shall appoint a senior officer to act as the chief AML/CFT compliance officer and vest the officer full authority in coordinating and supervising AML/CFT implementation and shall ensure that its AML/CFT personnel and the chief AML/CFT compliance officer do not hold concurrent positions
3	Whether the bank's internal rules and operating procedures for AML/CFT specify matters charged by the dedicated compliance unit or the chief AML/CFT compliance officer and whether there is the practice of assigning a unit or officer other than the dedicated compliance unit or chief AML/CFT compliance officer to take charge of the related matters.	that may have a conflict of interest with their AML/CFT responsibilities. In addition, a domestic bank shall set up an independent, dedicated AML/CFT compliance unit under the president, legal compliance unit, or risk management unit of the head office and such AML/CFT compliance unit shall not handle businesses other than AML/CFT. 」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
4	Aside from the duties of dedicated compliance unit or chief AML/CFT compliance officer stipulated by the FSC regulations, whether the bank clearly defines the division of works relating to AML/CFT among the dedicated compliance unit and respective business units. For example, when the Investigation Bureau requests customer information from the bank on a suspicious money laundering case	2. 2nd subparagraph, 1st paragraph

No.	Examination Item	Legal Basis
5	that the Bureau is investigating and the bank has set out in its internal rules and operating procedures the mechanism for re-inspecting the risk level of customer involved in the investigated case, are the works of replying to the Investigation Bureau and re-inspecting the customer risk level clearly specified or missed being mentioned; for detected suspicious money laundering transactions, is the division of labor for related investigation works clearly specified? The examiner should also make sampling check whether the actual operation is consistent with the contents of relevant internal rules and operating procedures. The examiner should make an overall judgment whether the bank has allocated adequate AML/CFT compliance personnel and resources based on the bank's risk profile, size, business characteristics, matters actually handled by the dedicated compliance unit, information system, database and training program that may be needed to assist in the detection of unusual transactions.	of Article 7「The dedicated AML/CFT compliance unit or the chief AML/CFT compliance officer mentioned in the preceding paragraph shall be charged with the 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 company-wide AML/CFT risk identification and assessment. 3. Monitoring and controlling ML/TF risks. 4. Developing an AML/CFT program. 5. Coordinating and supervising the implementation of AML/CFT program. 6. Confirming compliance with AML/CFT regulations, including the relevant specimen or self-regulatory rules formulated by the related financial services association and accepted by the FSC for recordation. 7. Supervising the reporting on suspicious ML/TF transactions and on the properties or property interests and location of individuals or legal entities designated by the Counter-Terrorism Financing Act

No.	Examination Item	Legal Basis
		to the Investigation Bureau, Ministry of Justice.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission 3. 2nd paragraph of Article 32「The chief compliance officer at a financial holding company or the head office of a banking business that is not governed by the foregoing paragraph cannot be appointed to internal posts other than chief legal officer or chief AML/CFT compliance officer, except as otherwise provided by the competent authority with respect to the credit cooperatives and bills finance companies.」, Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries (September 23, 2021 Amended) , Financial Supervisory Commission 4. Article 2「Financial institutions shall appoint a chief compliance officer to coordinate and supervise compliance with these Regulations.」,Regulations Governing Reporting on the

No.	Examination Item	Legal Basis
		Properties or Property Interests and Locations of Designated Sanctioned Individuals or Entities by Financial Institutions (November 14 ,2018 Amended), Financial Supervisory Commission
6	Whether the chief AML/CFT officer, AML/CFT compliance unit personnel and AML/CFT supervisor of domestic business units meet the qualification requirements.	2nd paragraph of Article 9 「The chief AML/CFT compliance officer, the personnel of dedicated AML/CFT unit and the AML/CFT supervisors of domestic business units of a banking business and other financial institutions designated by the FSC shall possess one of the following qualification requirements in three (3) months after appointment/assignment to the position and the financial institution shall set out relevant control mechanism to ensure compliance with the provisions hereof: 1. Having served as a legal compliance officer or AML/CFT personnel on a full-time basis for at least three (3) years; 2. Having attended at least 24 hours of courses offered by institutions recognized by the FSC, passed the exams, and received completion certificates therefor. But personnel who have met the qualification requirement for the legal compliance officer are deemed to meet the qualification requirement under this Subparagraph after they have attended at least 12 hours of

No.	Examination Item	Legal Basis
		training on AML/CFT offered by institutions recognized by the FSC; or 3. Having received an AML/CFT professional certificate issued by an international or a domestic institution recognized by the FSC.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
7	Whether the hours of training received by the chief AML/CFT officer, AML/CFT compliance unit personnel, AML/CFT supervisor of domestic business units, and AML/CFT supervisor and AML/CFT compliance officer of foreign business units meet the requirements.	3rd and 4th paragraph of Article 9 「The chief AML/CFT compliance officer, AML/CFT personnel and the AML/CFT supervisor of domestic business units of a banking business and other financial institutions designated by the FSC shall annually attend at least 12 hours of training on AML/CFT offered by internal or external training units consented by the chief AML/CFT compliance officer mentioned in Paragraph 1of Article 7herein.The training shall cover at least newly amended laws and regulations, trends and typologies of ML/TF risks. If the person has obtained an AML/CFT professional certificate issued by an international or a domestic institution recognized by the FSC in a year, the certificate may be used to substitute the training hours for the year.

No.	Examination Item	Legal Basis
		The AML/CFT supervisor and the AML/CFT compliance officer and personnel of foreign business units of a banking business and other financial institutions designated by the FSC shall possess professional knowledge on AML/CFT, be well informed in relevant local regulations, and annually attend at least 12 hours of training on AML/CFT offered by foreign competent authorities or relevant institutions. If no such training is available, the personnel may attend training courses offered by internal or external training units consented by the chief AML/CFT compliance officer mentioned in Paragraph 1 of Article 7herein.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
8	Whether the bank's chief AML/CFT compliance officer understand ML/FT risks associated with the bank's products and services, customers and geographic location, and has sufficient professional knowhow.	
9	If the AML/CFT compliance officer of a foreign business unit holds concurrent posts, is the situation reported to the FSC for record?	1. 4th paragraph of Article 7「Each foreign business unit of a banking business and other financial institutions designated

No.	Examination Item	Legal Basis
		by the FSC shall be staffed with an adequate number of AML/CFT personnel in view of the number of branches in that area, and the size and risks of its business, and appoint an AML/CFT compliance officer to take charge of the coordination and supervision of related compliance matters.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission 2. 4th paragraph of Article 32 「The compliance unit of the head office, domestic and foreign business units, information unit, assets safekeeping unit, and other management units of a financial holding company or a banking business shall each assign the personnel to act as the compliance officer to take charge of related affairs. Arranging the compliance officer position in the foreign business unit shall comply with the local regulations and the requirements of the local authorities and the compliance officer should not hold other

No.	Examination Item	Legal Basis
		posts except in any of the following situations: 1.The compliance officer serves concurrently as the AML/CFT compliance officer. 2.The compliance officer holds concurrent posts that do not constitute a conflict of interest according to the local regulations. 3.It is not strictly prohibited in the local regulations regarding the holding of concurrent posts, provided the holding of concurrent pots does not result or potentially result in conflict of interest and the matter has been communicated with and confirmed by the local competent authority and reported to the competent authority for recordation.」, Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries (September 23, 2021 Amended), Financial Supervisory Commission 3. 5th paragraph of Article 7 「The appointment of an AML/CFT compliance officer by the foreign business unit of a banking business and other financial institutions designated by the FSC shall comply with the regulations and requirements of

No.	Examination Item	Legal Basis
		the host country. The AML/CFT compliance officer shall be vested with full authority in AML/ CFT coordination and supervision, including reporting directly to the chief AML/CFT compliance officer mentioned in Paragraph 1 hereof, and shall not hold other positions, except for the legal compliance officer. If the AML/CFT compliance officer holds other concurrent positions, the foreign business unit shall communicate the fact with the competent authority of the host country to confirm the holding of other concurrent positions not resulting in or potentially leading to the conflict of interest, and report the matter to the FSC for recordation.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
(C)	Overseas branches and subsidiaries	
1	Whether a bank with foreign branches and/or subsidiaries has established an group-level AML/CFT program (applicable to overseas branches and subsidiaries as well), and established internal rules and	1. 4th paragraph of Article 6「A banking business and other financial institutions designated by the FSC having branches (or subsidiaries) shall establish a group-wide AML/CFT program

No.	Examination Item	Legal Basis
	operating procedures for information sharing within the group on condition that the regulatory requirements on data confidentiality of R.O.C. and jurisdictions where the bank has any foreign branch or subsidiary are met, and for requiring foreign branches and subsidiaries to provide customer, account and transaction information as well as safeguards on the confidentiality and use of information exchanged based on the group-level compliance, audit, and AML/CFT functions.	which shall be applicable, and appropriate to, all branches (or subsidiaries) of the financial group. The AML/CFT program shall include the policies, procedures and controls mentioned in the preceding paragraph, and in addition, contain the following without violating the information confidentiality regulations of the ROC and host countries or jurisdictions: 1. Policies and procedures for sharing information within the group required for the purposes of CDD and ML/TF risk management; 2. Group-level compliance, audit and AML/CFT functions to require branches (or subsidiaries) to provide customer, account and transaction information from branches and subsidiaries when necessary for AML/CFT purposes. This should include information and analysis of transactions or activities which appear unusual. Similarly branches (or subsidiaries) should receive such information from these group-level functions when necessary for AML/CFT purposes; and 3. Adequate safeguards on the confidentiality and use of

No.	Examination Item	Legal Basis
		information exchanged, including safeguards to prevent tipping-off.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission 2. 10th paragraph of Article 8「Financial holding companies and banking businesses shall establish a group-level AML/CFT program, which shall include intra-group information sharing policies and procedures for AML/CFT purposes, based on the laws and regulations of countries or jurisdictions where the foreign branches (or subsidiaries) are located.」, Implementation Rules of Internal Audit and Internal Control System of Financial Holding Companies and Banking Industries (September 23, 2021 Amended), Financial Supervisory Commission 3. 2nd paragraph of Article 17「Employed personnel prescribed in paragraphs 1 to 3 of Article 5, who are not public officials, and who disclose or deliver documents, pictures, information or objects relating to

No.	Examination Item	Legal Basis
		reported transactions suspected of violating provisions under Articles 14 and 15, or to suspected offences described in Articles 14 and 15, will f shall be sentenced to imprisonment of not more than two year, a detention, or a fine of not more than NT$500,000.」, Money Laundering Control Act (November 7, 2018 Amended), Ministry of Justice
2	Examine the group-level AML/CFT program established by the bank to determine whether it contains supervision and management of ML/TF risks faced by its foreign branches and subsidiaries. For example, does the head office have the channel or means to output and analyze in a timely manner relevant MIS reports on foreign branches and subsidiaries to monitor periodically their business activities and monitor whether the red flags or filtering indicators of suspicious transactions used by the branch or subsidiary are commensurate with its business activities; whether the bank has established a mechanism to readily understand and supervise compliance with the local laws and regulations by the foreign branches and subsidiaries, and for weaknesses or deficiencies in the AML/CFT program of a foreign branch or subsidiary identified by the foreign	

No.	Examination Item	Legal Basis
	competent authority or in self-inspection or internal audit unit, whether there is a mechanism to inform the board of directors or senior management based on the risk level of the weakness or deficiency.	
3	Examine the daily AML/CFT management reports on the business activities of foreign branches and subsidiaries outputted by the head office, head office's analysis or conclusions on the reports and the risk assessment data of foreign branches and subsidiaries to confirm that the head office carries daily supervision and management of its foreign branches and subsidiaries (in particularly branches and subsidiaries that operate in high ML/TF risk jurisdictions or offer high-risk products or services to customers).	
4	Examine the bank's internal rules and operating procedures for group-level information sharing and whether the bank has assessed the legality of the scope and mechanism of information sharing with supporting evidence attached (regulations of the host country or relevant legal opinions). For example, according to the R.O.C. Money Laundering Control Act, the internal rules and operating procedures for information sharing within the group of a financial institution may not include reported suspicious transaction cases, whereas according to the Interagency	

No.	Examination Item	Legal Basis
	Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies of the U.S. Department of the Treasury, a financial information may share filed suspicious activity reports with its head office or controlling company outside the United States, but there must have written confidentiality agreements or arrangements in place specifying that the head office or controlling company must protect the confidentiality of the suspicious activity reports through appropriate internal controls.	
5	Examine the bank's internal rules and operating procedures for group-level information sharing to evaluate whether the scope of sharing is reasonable. For example, if it is unlikely for a customer to carry out transactions at a foreign branch or subsidiary, the information on the customer should be excluded from the scope of sharing. However on condition that it is legal to do so, if a customer has been declined by the head office (or a foreign branch or subsidiary) to open an account, information on the denied account may be shared with foreign branches and subsidiaries (head office), or information on common customers should be shared within the group, particularly regarding high-risk customers to effectively assess and understand customer risk and	

No.	Examination Item	Legal Basis
	facilitate monitoring and controlling unusual transactions within the group.	
6	If a foreign branch or subsidiary is unable to share the identity, account and transaction information of customers with the head office (group) due to local regulations, does the bank or the foreign branch or subsidiary provide a legal opinion or local regulations to corroborate the reason for non-compliance (including the types of information that cannot be provided)? The bank should also describe in its AML/CFT program the foreign branches and subsidiaries that are unable to comply with the information sharing requirements, analyze the impact thereof and reflect it in its risk assessment result.	
7	The examiner should check whether the customer information actually shared between the head office and its foreign branches and subsidiaries outstep the regulatory restrictions and the established rules.	
8	The examiner on information business should understand the confidentiality of channels or means used by the head office and foreign branches and subsidiaries in transmitting and storing relevant information.	
9	Whether the bank's foreign branches and subsidiaries apply AML/CFT measures, to the extent that the laws and regulations of host countries or	5th subparagraph of Article 6「A banking business and other financial institutions designated by the FSC shall ensure that its foreign branches

No.	Examination Item	Legal Basis
	jurisdictions so permit, consistent with the home country requirements; the examiner should check the internal rules and operating procedures of the foreign branches and subsidiaries for AML/CFT, examination reports of foreign regulators and relevant documents to understand the actual practices of the foreign branches and subsidiaries. In particular the examiner should check the examination opinions given by foreign regulators to corroborate whether the foreign branch or subsidiary has implemented AML/CFT measures consistent with those adopted by the head office. Unless the host country has stricter regulations, if there is any inconsistency, the examiner should find out whether the inconsistency is caused by the lack of supervision on the part of the head office making sure its foreign branches and subsidiaries apply the same criteria as the head office.	(or subsidiaries) apply AML/CFT measures to the extent that the laws and regulations of host countries or jurisdictions so permit, and those measures should be consistent with those adopted by the head office (or parent company). Where the minimum requirements of the countries where its head office (or parent company) and branches (or subsidiaries) are located are different, the branch (or subsidiary) shall choose to follow the criteria which are higher. However, in case there is any doubt regarding the determination of higher or lower criteria, the determination by the competent authority of the place at where the head office of the banking business and other financial institutions designated by the FSC is located shall prevail. If a foreign branch (or subsidiary) is unable to adopt the same criteria as the head office (or parent company) due to prohibitions from foreign laws and regulations, appropriate additional measures shall be taken to manage the ML/TF risks, and report to the FSC. 」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission

No.	Examination Item	Legal Basis
(D)	AML/CFT program effectiveness audit (independent testing)	1st and 2nd paragraph of Article 8 「Each domestic and foreign business unit of a banking business and other financial institutions designated by the FSC shall appoint a senior manager to act as the supervisor to take charge of supervising AML/CFT related matters of the business unit, and conduct self-inspection. The internal audit unit of a banking business and other financial institutions designated by the FSC shall audit the following matters and submit audit opinions on: 1. Whether the ML/TF risk assessment and the AML/CFT program meet the regulatory requirements and are implemented; and 2. The effectiveness of the AML/CFT program.」, Regulations Governing Internal Audit and Internal Control System of Anti-Money Laundering and Countering Terrorism Financing of Banking Business and Other Financial Institutions Designated (December 14, 2021 Announced), Financial Supervisory Commission
1	Examine whether the internal audit unit of the bank that conducts AML/CFT program effectiveness audit possesses independence. For example, the internal audit unit is not involved in the AML/CFT risk assessment or setting the red flags and thresholds for suspicious transactions.	
2	Evaluate the qualifications of internal auditors who perform effectiveness audit to assess whether the bank or the financial supervisory agency can rely on their findings and conclusions.	
3	Examine the report and work-papers produced by the internal audit unit to determine whether the scope of audit is comprehensive, adequate and timely; effectiveness audit performed by the internal audit unit includes but is not limited to the following: ①The adequacy, effectiveness and regulatory compliance of the overall content of the bank's internal rules and operating procedures for AML/CFT; the information contained in the internal audit report and working papers should be as comprehensive as possible for examination and judgment by external units. ②Audit whether the bank's ML/TF	

No.	Examination Item	Legal Basis
	risk assessment result is reasonable based on the bank's risk profile (customer, product, service, geographic location, etc.). ③Conduct transaction testing using a risk-based approach to verify that relevant reporting and record-keeping comply with the regulatory requirements, and whether staff are performing their jobs in accordance with the internal rules and operating procedures for AML/CFT. ④ Audit whether the training arranged by the bank for bank-wide personnel (in-house or outside training) is comprehensive, whether the training materials contain errors and whether attendance is normal. ⑤ Follow up on the deficiencies found in the previous internal audit report or the examination report of the financial supervisory agency to see if those deficiencies have been remedied or remedial actions have been taken according to the timetable.	
4	Examine whether the audit of suspicious ML/TF monitoring system (information and/or manual assistance) by the internal audit unit includes an evaluation of the system's ability to identify suspicious transactions; confirm through a validation of internal audit report and related work-papers that audit	

No.	Examination Item	Legal Basis
	conducted by the internal audit unit includes the following: ① Review whether the bank's internal rules and operating procedures for suspicious transaction monitoring mechanism adequate. For example, manual identification and reporting procedures for suspicious transaction, and investigation and handling procedures for suspicious transactions. ②Determine whether the filtering or screening indicators set by the bank are reasonable and cover all self-identified higher-risk products, services, customers or geographies. ③Determine whether the filtering or screening indicators set by the MIS system that assists the bank in identifying suspicious transactions are complete and accurate, and whether the MIS system can generate comprehensive and accurate monitoring reports. ④Determine whether filing of STR by the bank is timely and whether the report contents are comprehensive and accurate.	
5	Evaluate the adequacy of internal audit based on the following: ① Overall audit coverage and frequency in relation to the bank's risk profile. For example, whether the risk-based effectiveness audit plan drawn up by the internal	

No.	Examination Item	Legal Basis
	audit unit covers all bank business units (including overseas branches and subsidiaries) and whether the depth of audit is planned based on risk. ②Whether internal audit unit plans depth of audit based on risk and whether the audit and testing of monitoring mechanism, particularly for high-risk operations (products and services) and suspicious transaction is adequate. ③ The competency of internal auditors who conduct AML/CFT effectiveness audit.	
6	When necessary, the examiner can carry out validation based on the following procedures: ①Higher-risk products and services, customer and entities, and geographic locations for which it appears from the scoping and planning process that the bank may not have appropriate internal controls, and new products and services, customers and entities, and geographies introduced into the bank's portfolio since the previous AML/CFT examination ②Select a sample of cases from the aforementioned scope that differ from the cases audited by the internal audit unit to determine whether the effectiveness testing conducted by the internal audit unit is comprehensive and adequate, whether the internal	

No.	Examination Item	Legal Basis
	audit unit has audited the accuracy of suspicious transaction monitoring system, the ability of the monitoring system to identify suspicious transaction, and suspicious transaction verification and reporting procedures.	
F	Countering Financing Terrorism The Terrorist Financing report issued by FATF in 2008 indicates that terrorists and terrorist groups use a wide variety of financial instruments (e.g. cash, ATMs, credit cards, currency exchange, remittances, loans, new payment tools, online banking, and mobile payments), but non-profit organizations are relatively vulnerable to terrorism financing, and in higher-risk regions there are military conflicts, terrorist groups are very active, and there are countries and regions that finance terrorism or are non-cooperative with efforts to combat the financing of terrorism. Auditors can adopt the following procedures to audit a bank's implementation of CFT measures.	
(A)	Comprehensiveness of information on originators and beneficiaries (For information on examination items, please refer to "4. Policies and procedures", "(2) Effectiveness of internal controls", "1. Wire Transfer Business".)	
(B)	Screening of sanctions lists using fuzzy matching	
1	The entity list created pursuant to	1.8th subparagraph of Article 4 「The

No.	Examination Item	Legal Basis
	United Nations Security Council Resolutions 1267, 1989, 2253, and 1988, and terrorists or terrorist groups which the bank has blacklisted and have been identified or investigated by a foreign government or an international anti-money laundering organization must be examined on a random sample basis to check whether the bank's name list is complete and kept promptly up to date.	customer is an individual, a legal person or an organization sanctioned under the Terrorism Financing Prevention Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization, except for payments made under Subparagraphs 1 ~ 3, Paragraph 1, Article 6 of the Terrorism Financing Prevention Act」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended),Financial Supervisory Commission
2	Use a modified sanctions list to test the effectiveness of the bank system's fuzzy matching function. (For information on other related audit procedures, including checking for successful matches during list screening and the suitability of handling procedures, please refer to: "2. Customer due diligence", "(3) Screening of customer names"; to test the bank system's parameter settings, refer to "Appendix 4, Screening logic".)	2. Article 8「Financial institutions shall observe the following provisions in watch list filtering: 2.A financial institution shall establish policies and procedures for watch list filtering, using a risk-based approach, to detect, match and filter whether customers, or the senior managerial officers, beneficial owners or trading counterparties of customers are individuals, legal persons or organizations sanctioned under the Terrorism Financing Prevention Act or terrorists or terrorist groups identified or investigated by a foreign government or an international anti-money

No.	Examination Item	Legal Basis
		laundering organization. 2. The policies and procedures for watch list filtering shall include at least matching and filtering logics, implementation procedures and evaluation standards, and shall be documented. 3. A financial institution shall document its name and account filtering operations and maintain the records for a time period in accordance with Article 12 herein. 」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended),Financial Supervisory Commission
(C)	Assess whether the bank carries out customer due diligence measures to identify and verify the identity of the beneficial owners of legal-person customers that carry out transactions. (For information on examination items, please refer to: "2. Customer due diligence".)	
(D)	Assess whether the bank conducts enhanced measures (and the adequacy of any such measures) with respect to: (i) transactions involving non-profit organizations that are relatively vulnerable to terrorism financing and have been assessed as high risk; and (ii) transactions involving higher risk regions (i.e. regions where there is armed conflict, regions where terrorist organizations are active, and	

No.	Examination Item	Legal Basis
	countries and regions that finance terrorism or are non-cooperative with efforts to combat the financing of terrorism).	
(E)	Review the adequacy of the bank's policies and procedures for the reporting and freezing of properties or property interests of designated sanctioned individuals or entities. (Please refer to "Appendix E, FAQs on Banks' Implementation of the Counter-Terrorism Financing Act".)	
G	Countering Financing Proliferation The Proliferation Financing Report issued by the FATF in 2008 states that trade finance services present relatively high risk of being abused for proliferation financing with financial services and products such as letters of credit, documentary collections, and clean payments (i.e. open account and payment in advance). The examiner can adopt the following procedures to audit a bank's implementation of measures to prevent proliferation financing.	
(A)	Comprehensiveness of information on originators and beneficiaries (For information on examination items, please refer to "4. Policies and procedures", "(2)Effectiveness of internal controls", "1. Wire Transfer Business".)	
(B)	Screening of sanctions lists using fuzzy matching	1.8th subparagraph of Article 4 「The customer is an individual, a legal person or an organization sanctioned under the Terrorism
1	The entity list created pursuant to United Nations Security Council	

No.	Examination Item	Legal Basis
	Resolution 1718 (and follow-on resolutions 1874, 2087, 2094, 2270, 2231, 2356, 2371, 2375, and 2397) and Resolution 2231 must be examined on a random sample basis to check whether the bank's name list is complete and kept promptly up to date.	Financing Prevention Act, or a terrorist or terrorist group identified or investigated by a foreign government or an international anti-money laundering organization, except for payments made under Subparagraphs 1 ~ 3, Paragraph 1, Article 6 of the Terrorism Financing Prevention Act」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended),Financial Supervisory Commission
2	Use a modified sanctions list to test the effectiveness of the bank system's fuzzy matching function. (For information on other related examination items, including checking for successful matches during list screening and the suitability of handling procedures, please refer to: "2. Customer due diligence", "(3) Screening of customer names"; to test the bank system's parameter settings, refer to "Appendix D, Screening logic".)	2. Article 8「Financial institutions shall observe the following provisions in watch list filtering: 2.A financial institution shall establish policies and procedures for watch list filtering, using a risk-based approach, to detect, match and filter whether customers, or the senior managerial officers, beneficial owners or trading counterparties of customers are individuals, legal persons or organizations sanctioned under the Terrorism Financing Prevention Act or terrorists or terrorist groups identified or investigated by a foreign government or an international anti-money laundering organization. 2. The policies and procedures for watch list filtering shall include at

No.	Examination Item	Legal Basis
		least matching and filtering logics, implementation procedures and evaluation standards, and shall be documented. 3. A financial institution shall document its name and account filtering operations and maintain the records for a time period in accordance with Article 12 herein. 」, Regulations Governing Anti-Money Laundering of Financial Institutions (December 14, 2021 Amended),Financial Supervisory Commission
(C)	Assess whether the bank carries out customer due diligence measures to identify and verify the identity of the beneficial owners of legal-person customers that carry out transactions. (For information on audit procedures, please refer to: "2. Customer due diligence".) Note whether the customer has any factors involving North Korea (e.g. whether the account's authorized signatories, contact persons, contact address, etc. have any connection to DPRK.)	
(D)	Assess the adequacy of the bank's policies and procedures for identifying high-risk customers and transactions. Factors that could support a determination whether the related transactions are suspicious of sanction evasion include the following: there are proliferation financing concerns regarding the	

No.	Examination Item	Legal Basis
	entities involved in transactions, and the goods, raw materials, equipment, or technologies involved in transactions involve arms manufacturers; financial transactions involve proliferation financing typologies and red flags (please refer to "Appendix F, Potential Indicators of Proliferation financing from FATF Guidance on Counter Proliferation Financing"); persons related to transactions are involved in some way with a list of persons who have been denied export licenses (including the reasons for denial and the goods involved).	
(E)	Check whether the bank, depending on the circumstances surrounding particular transactions, collects additional information on high-risk customers and transactions in order to conduct enhanced scrutiny (including ongoing monitoring) and determine whether the related transactions are suspicious of sanction evasion. The additional information that could be collected might include the following: 1. Purpose of transaction or payment of funds; 2. The end user or ultimate use of any goods; 3. Transaction counterparty; 4. Source of funds; 5. Information on goods controls; 6. Completeness and accuracy of information on inward	

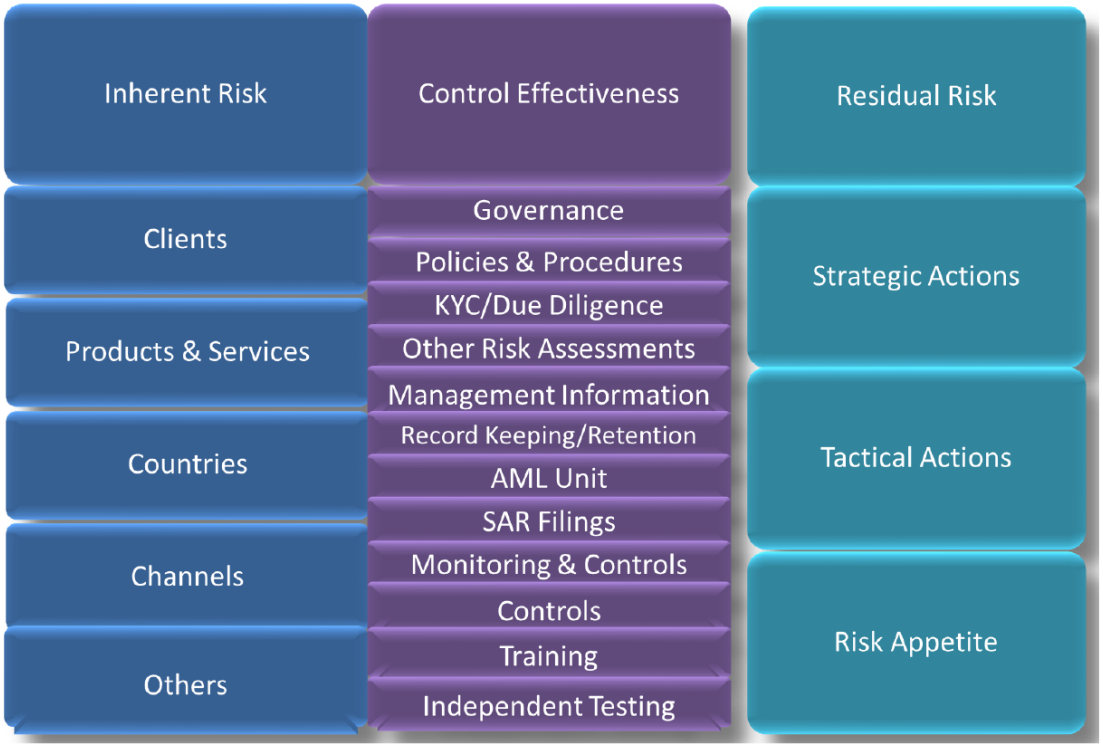
No.	Examination Item	Legal Basis
	remittances; 7. Whether the customer's transaction counterparties or beneficial owners are involved in representing either North Korean financial institutions or persons or groups designated by North Korean financial institutions, or are offshore company's controlled by North Korea; 8. For customers that are diplomats at North Korean embassies (including all embassy employees and all close associates of all diplomatic personnel), conduct enhanced scrutiny and properly implement the requirements of UN Security Council Resolution 2321 (2016).	
(F)	Check whether the bank has entered into any correspondent bank, remitting bank, RMA, or credit relationship with a North Korean financial institution.	
(G)	Examine the bank's outward and inward remittances over a specific period and screen for open account transactions to check whether the originator is clearly a remittance firm or a front company, whether the export goods of the customer (the recipient of an inward remittance) are the principal export goods of the originator's country or region, whether there is a clear inconsistency between the attributes of the businesses run by the recipient and	

No.	Examination Item	Legal Basis
	the originator, whether the bank has a system for due diligence when industrial goods are purchased using an individual's account (the bank may carry out due diligence either during or after transactions, depending on its own needs) to understand whether the transactions , and whether the bank has established a policy on when to accept or refuse transactions.(Please refer to "Appendix F, Potential indicators of proliferation financing from FATF Guidance on Counter Proliferation Financing ".)	
(H)	Examine the bank's trade finance transactions over a specific period to check whether there are irregularities, whether the bank conducts due diligence when irregularities occur (for information on audit procedures, please refer to "4. Policies and procedures", "(2) Effectiveness of internal controls", "6. Trade finance"), and whether the bank has established a policy on when to accept or refuse transactions.	
(I)	Review the adequacy of the bank's policies and procedures for the reporting and freezing of properties or property interests of designated sanctioned individuals or entities. (Please refer to "Appendix E, FAQs on Banks' Implementation of the Counter-Terrorism Financing Act".)	

Appendix A Risk Assessment Framework[1]

(A) 3 Phases of Risk Assessment

While there are numerous ways to conduct Risk Assessments, increasingly the most common approach used by FIs can be described as the "conventional/standard methodology." The following diagram illustrates what might be expected in practice, although this may clearly vary from one FI to another:



The risk assessment should cover the entirety of the FI's business, though may be conducted in parts, or as part of a rolling cycle, to focus on separate areas, such as divisions, units or specific business lines, countries and/or legal entities. The risk assessment should consider all relevant inherent money laundering risk factors in order to determine its risk profile and in turn assess the nature of mitigating controls, both from a design and operating effectiveness standpoint, in order to arrive at the residual risk, which should be within the FI's established risk appetite. While the risk assessment is the responsibility of the FI as a whole, the money laundering risk assessment will usually be designed and carried out by the competent AML Unit, applying specialist knowledge and expertise alongside the gathering of relevant external and internal information. The risk assessment process can be considered in 3 Phases:

Phase 1: Determine the Inherent Risk;

Phase 2: Assess the Internal Control Environment (both design and operating effectiveness); and Phase 3 Derive the Residual Risk.

[1] Information Source: Wolfsberg FAQ on Risk Assessment for ML, Sanctions and Bribery & Corruption, 2015

(B)Example Process for a Risk Assessment

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

1. Define the inherent risk factors

2. Weight the inherent risk factors as per methodology

3. Collect the data and subject it to appropriate review

4. Score the inherent risk factors to arrive at both

a. an individual risk category rating, e.g. High, Moderate, Low (HML); and

b. an overall HML score

5. Define the control effectiveness categories

6. Identify all the controls and map either to:

a. the Controls categories:

i. Weight the Categories based on importance, number of controls, number of key controls; and

ii. Score the control effectiveness by aggregating the results to get an overall HML score; OR

b. the Inherent risk categories:

i. Weight the controls based on importance, key Controls.

ii. Map the Controls to each of the Inherent risk categories and score those controls in aggregate against each risk category; and

iii. Aggregate the control effectiveness categories to get an overall HML score;

7. Note and record the shortcomings or weaknesses in each of the identified controls for future remediation work (see 10 below)

8. Take the overall inherent risk score and apply the controls effectiveness score by applying the residual risk matrix

9. Arrive at the residual risk and determine at the appropriate governance body whether the residual risk is within FI tolerance or risk appetite; and

10. Determine the remediation action plan covering those items in 8 above that are determined as being in need of further action, by whom and by when.

Note:

Given the above methodology, certain rules can be adopted within a ML risk assessment when finalising risk ratings, for example:

i) A Strong control environment can lower the residual ML risk in comparison to the inherent risk;

ii) If the FI/business unit/business line receives a High rating of inherent ML risk, it can never achieve a residual ML risk rating of Low; and

iii) In order to improve its residual ML risk, either the inherent ML risk can be reduced or the

AML controls can be strengthened.

Appendix B Red Flags for Suspicious Money Laundering or Terrorism Financing Transactions

Approved by the Financial Supervisory

Commission, with Letter Chin-Kuan-Yin-Fa-Tze

10610003210 dated June 28, 2017

1. Products / Services – Deposit, Withdrawal, or Remittance
   (1) The aggregation of cash deposited into an account, or the aggregation of cash withdrawn from an account, reaches a specific amount within a certain period.
   (2) The aggregation of cash deposited into a customer's accounts, or the aggregation of cash withdrawn from a customer's accounts, reaches a specific amount within a certain period.
   (3) The aggregation of cash deposited by a customer, or the aggregation of cash withdrawn by a customer, with the amount of each transaction slightly below the currency reporting threshold, reaches a specific amount within a certain period.
   (4) A customer's account suddenly has deposits that accumulatively reach a specific amount (e.g. by depositing multiple promissory notes or checks into the account.)
   (5) An inactive account suddenly has deposits that accumulatively reach a specific amount and are transferred rapidly.
   (6) Immediately after a customer opens an account, payments that accumulatively reach a specific amount are deposited or remitted into the account and transferred rapidly.
   (7) Payments are intensively deposited into an account and transferred rapidly to the extent that the total amount or number of payments reaches a specific level.
   (8) A customer frequently transfers funds that accumulatively reach a specific amount between multiple customer accounts.
   (9) A customer frequently processes transactions in the form of cash withdrawal but such transactions have an effect of money transfer.
   (10) Each of a customer's deposit is followed immediately by a withdrawal with

similar amount, and such transactions accumulatively reach a specific amount.

(11) A customer frequently deposits or withdraws cash on behalf of other person, or an account is frequently deposited or withdrawn cash by a third party, to the extent that such transactions accumulatively reach a specific amount.

(12) A customer uses cash that accumulatively reaches a specific amount at a time to make multiple remittances or apply negotiable instruments (e.g. cashier's checks, due-from-bank checks and drafts), negotiable certificates of deposit, traveler's checks, beneficiary certificates, or other securities.

(13) A customer purchases or sells foreign exchange, foreign currency cash, traveler's checks, foreign currency drafts, or other bearer's financial instruments that accumulatively reach a specific amount.

(14) A customer frequently exchanges small-denomination notes for those of large-denomination, or vice versa.

(15) The funds remitted from or to high ML/TF risk jurisdictions accumulatively reach a specific amount. The high ML/TF risk jurisdictions described in the Template include but are not limited to the jurisdictions, published by international anti-money laundering organizations and notified by Financial Supervisory Commission, 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. Products / Services – Credit

(1) A customer suddenly repays loans that accumulatively reach a specific amount but fails to reasonably explain the source of funds.

(2) A customer uses large amount of cash, cash equivalents, high-value goods, or real estates, etc., or funds, assets or credits provided by unrelated third-parties as collaterals or guarantees to apply loans.

(3) Default on loans secured by cash, cash equivalents, or assets that can be easily converted into cash with the intention of having bank dispose such collaterals.

3. Products / Services – Offshore Banking Unit
   (1) Within a certain period, multiple domestic residents receive remittance from an offshore account, and the transfer and settlement of funds are operated by one or a small number of persons.
   (2) An account is operated in the name of an offshore company or an offshore account held by a foreign legal person or individual is operated by a domestic enterprise, with regular movement of funds that accumulatively reaches a specific amount within a certain period.
   (3) A customer builds up large balances in an account and frequently transfers funds that accumulatively reach a specific amount to the customer's offshore account(s).
   (4) A customer frequently deposits traveler's checks and foreign currency drafts that are issued overseas.
   (5) Within a certain period, a customer frequently purchases large amounts of offshore structured products, which are inconsistent with the customer's needs.

4. Products / Services – Trade Finance
   (1) Discrepancies appear between the description of the commodity on the bill of lading and payment order or invoice, such as inconsistency in the product amount or type.
   (2) Significant discrepancies appear between the pricing or the value of the product or service reported on the invoice and its fair market value (undervalued or overvalued).
   (3) The method of payment appears inconsistent with the risk characteristics of the transaction, for example, the use of an advance payment for a new supplier in a high-risk jurisdiction.
   (4) A transaction involves the use of letters of credits that are amended, extended, or change payment location frequently or significantly without a reasonable explanation.
   (5) Using letters of credit, negotiable instruments or other means that are issued overseas without trade basis to obtain financing.
   (6) Commodities shipped are inconsistent with the customer's industry or operations, or unrelated to the customer's business nature.

(7) Customers involved in high-risk suspicious ML/TF activities, including importing/exporting goods that are subject to embargo or restrictions (e.g., military supplies of foreign governments, weapons, chemicals, or natural resources such as metals).

(8) The commodity is shipped to or from a high ML/TF risk jurisdiction.

(9) The type of commodity shipped is vulnerable to ML/TF, for example, high-value but low-volume goods (such as diamonds and artworks).

5. Products / Services – Correspondent Banking

(1) The amount of credits and debits in an account held by a financial institution is apparently inconsistent with its scale of deposit or nature of business, or the fluctuations of credits and debits in such account apparently exceeds the fluctuation of its deposits.

(2) Unable to identify the actual account holder of a payable-through account.

(3) The currency-shipment patterns with a respondent bank has a significant change.

(4) A respondent bank rapidly increases the amount and number of cash deposits while its non-cash deposits are not relatively increased.

6. Products / Services – Safe Deposit Box

(1) A customer uses safe deposit box in an unusual frequent manner. For example, a customer frequently opens safe deposit box or rents multiple safe deposit boxes.

(2) A customer opens safe deposit box with several individuals, or an individual that is not the original lessee frequently opens the safe deposit box.

7. Products / Services – Others

(1) Frequent fund transfer between a prepaid card company's accounts located in different jurisdictions accumulatively reaches a specific amount.

(2) Using personal accounts to conduct embassy, diplomatic representative office, or official affairs; or using accounts held by embassy, diplomatic representative office, or governments to pay personal expenses of foreign nationals (such as expenses for college students).

8. Unusual Transaction Activity / Behavior – Transaction Behavior

(1) Selling financial debts in large volume but requesting cash payments; frequently using traveler's checks or foreign currency checks that accumulatively reach a specific amount without a reasonable explanation; lacking reasonable information of the underlying trade's quantities and prices in the transactions of issuing letters of credit that accumulatively reach a specific amount; or opening an account with large amount cashier's checks issued by another financial institution but seems to be suspicious ML/TF transaction.

(2) Deposit, withdrawal, remittance, or other transactions conducted by an individual involved in a special and material case that is instantly reported by television, press, internet or other media are apparently unusual.

(3) Several individuals together go to a bank to conduct deposit, withdrawal, remittance, or other transactions.

9. Unusual Transaction Activity / Behavior – Customer identification information

(1) A customer has "Regulations Governing the Deposit Accounts and Suspicious or Unusual Transactions", "Template of Directions Governing Anti-Money Laundering and Combatting the Financing of Terrorism of Banks", or other circumstances that result in the incompletion of customer identification process.

(2) A large number of customers share the same address, occupants of an address change frequently, or the address is not the actual residence address.

(3) An originator of cross-border remittance fails to provide a reasonable explanation on the relationship between the originator and the beneficiary.

10. Terrorism Financing

(1) Related parties of a transaction are terrorists or terrorist groups designated by foreign governments and notified by Financial Supervisory Commission, or terrorist groups identified or investigated by an international organization; or the fund for a transaction seems to, or is reasonably suspected to, have a connection with terrorism activities,

groups, or terrorism financing.

(2) Within a certain period, a young customer either withdraws or transfers funds that accumulatively reach a specific amount, transfers or remit funds that accumulatively reach a specific amount to hot areas of frequent military and terrorism activities or non-profit organizations, and immediately terminates relationship or closes the account.

(3) Cross-border transactions that accumulatively reach a specific amount are conducted in the name of a non-profit organization without a reasonable explanation.

11. Cross-border Transactions

(1) A customer frequently transfers funds abroad that accumulatively reach a specific amount.

(2) A customer frequently transfers funds from abroad and immediate withdraws cash that accumulatively reaches a specific amount.

(3) A customer frequently receives funds from abroad that accumulatively reach a specific amount and immediate remit such funds to another person in the same jurisdiction, or to the original sender’s account in another jurisdiction.

(4) A customer frequently transfers funds from or to a jurisdiction that presents high risk of tax evasion or financial secrecy.

Appendix C On-site Requested Items

Appendix D Screening Logic

No	Factor	Matching rule & process rule	impact
1	upper/lower case	upper & lower case are treated as the same.	No impact
2	Apostrophe (')	Apostrophe will be ignored.	No impact
3	Slash or Back slash or a specific number + slash (e.g. 1/)	will be ignored	No impact
4	Bracket (())	Input name with bracket will eventually create two variation. 1) exclude bracket only 2) exclude bracket and all contnt within	No impact
5	Comma (,)	Will create a variation of name which will reverse the order of a name with a comma seperator.	No impact
6	Dot (.,)		No impact
7	Other symbols		No impact
8	Trivial word	Some of the common titles such as "Mr" and "Mrs" are considered as trivial words. Therefore, will be ignored.	No impact
9	Flipped first and last name		No impact

Appendix E FAQs on Banks' Implementation of the Counter-Terrorism Financing Act

Appendix F Potential indicators of proliferation financing from FATF Guidance on Counter Proliferation Financing

A. The following indicators of possible proliferation financing as mentioned in Annex 1 to the 2008 FATF Typologies Report on Proliferation Financing elements that may indicate proliferation financing are

(i) Transaction involves person or entity in foreign country of proliferation concern.

(ii) Transaction involves person or entity in foreign country of diversion concern.

(iii) The customer or counter-party or its address is similar to one of the parties found on publicly available lists of "denied persons"[2] or has a history of export control contraventions.

(iv) Customer activity does not match business profile, or end-user information does not match end-user's business profile.

(v) A freight forwarding firm is listed as the product's final destination. (vi) Order for goods is placed by firms or persons from foreign countries other than the country of the stated end-user.

(vii) Transaction involves shipment of goods incompatible with the technical level of the country to which it is being shipped, (e.g. semiconductor manufacturing equipment being shipped to a country that has no electronics industry).

(viii) Transaction involves possible shell companies (e.g. companies do not have a high level of capitalisation or displays other shell company indicators).

(ix) Transaction demonstrates links between representatives of companies exchanging goods i.e. same owners or management.

(x) Circuitous route of shipment (if available) and/or circuitous route of financial transaction.

(xi) Trade finance transaction involves shipment route (if available) through country with weak export control laws or weak enforcement of export control laws.

(xii) Transaction involves persons or companies (particularly trading companies) located in countries with weak export control laws or weak enforcement of export control laws.

(xiii) Transaction involves shipment of goods inconsistent with normal geographic trade patterns (e.g. does the country involved normally export/import good involved?).

(xiv) Transaction involves financial institutions with known deficiencies in AML/CFT

[2] Could refer to https://icp.trade.gov.tw/ICP/Display.action?pageName=OList

controls and/or domiciled in countries with weak export control laws or weak enforcement of export control laws.

(xv) Based on the documentation obtained in the transaction, the declared value of the shipment was obviously under-valued vis-à-vis the shipping cost.

(xvi) Inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination etc.

(xvii) Pattern of wire transfer activity that shows unusual patterns or has no apparent purpose.

(xviii) Customer vague/incomplete on information it provides, resistant to providing additional information when queried.

(xix) New customer requests letter of credit transaction awaiting approval of new account.

(xx) Wire instructions or payment from or due to parties not identified on the original letter of credit or other documentation.

B. The following additional potential indicators of sanctions evasion activity mentioned in third-party reports (e.g. UN PoE Reports, academic research)

(i) Involvement of items controlled under WMD export control regimes or national control regimes.

(ii) Involvement of a person connected with a country of proliferation concern (e.g. a dual-national), and/or dealing with complex equipment for which he/she lacks technical background.

(iii) Use of cash or precious metals (e.g. gold) in transactions for industrial items.

(iv) Involvement of a small trading, brokering or intermediary company, often carrying out business inconsistent with their normal business.

(v) Involvement of a customer or counter-party, declared to be a commercial business, whose transactions suggest they are acting as a money-remittance business.

(vi) Transactions between companies on the basis of “ledger” arrangements that obviate the need for international financial transactions.

(vii) Customers or counterparties to transactions are linked (e.g. they share a common physical address, IP address or telephone number, or their activities may be coordinated).

(viii) Involvement of a university in a country of proliferation concern.

(ix) Description of goods on trade or financial documentation is nonspecific, innocuous or misleading.

(x) Evidence that documents or other representations (e.g. relating to shipping, customs, or payment) are fake or fraudulent.

(xi) Use of personal account to purchase industrial items.