AML/CFT Compliance Examination Manual

for Banking Sector

Examination Item

A、Policies and Procedures

B、Customer Due Diligence

C、Ongoing Monitoring and Suspicious Transaction Report

D、Risk Prevention Program (Risk Assessment)

E、Organization and Personnel

No.	Examination Item
A	**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), which requires the board of directors and chief AML/CFT compliance officer to take charge of supervising AML/CFT risks and the AML/CFT program has been passed by the board of directors; whether the bank regularly 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.
2	Whether the relevant policies, procedures or documented internal rules (e.g. instructions, measures, guidelines, etc.) established by the bank cover customer due diligence (including verification of customer identity and watch list filtering), 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 mitigation measures (including ongoing monitoring of correspondent bank accounts and transactions).
3	Whether the bank's relevant unit reports non-compliance with internal AML/CFT related rules or operating procedures or major deficiencies (including deficiencies

No.	Examination Item
	of the 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.
4	Whether the board of directors and 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 internal controls and letting board members sufficiently understand the contents and meaning of AML/CFT report; has

No.	Examination Item
	relevant members signed and issued a statement on internal AML/CFT controls?
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?
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 or electronic form (e.g. through the system), retaining watch list filtering 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?
(B)	Effectiveness of internal controls The following businesses or lines of business are lines of business posing high AML/CFT risks, and products, services or customers of banking business vulnerable to money laundering and terrorist financing (ML/TF) identified in the National ML/TF Risk Assessment Report and businesses for which specific

No.	Examination Item
	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 in the aforementioned lines of business, 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 procedures and results for items under **"Customer Due Diligence", "Ongoing Monitoring and 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 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. When information on the trading counterparty is incomplete, the bank is unable to carry out properly monitoring of suspicious transactions and watch list filtering. 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 properly evaluate and

No.	Examination Item
	manage risks associated with remittance and settlement operations by monitoring suspicious transactions and carrying out watch list filtering. 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 mitigation measures: Obtaining customer due diligence (CDD) information is the most important risk mitigation 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. Banks must observe the wire transfer message format and carry out proper watch list filtering 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 details:
㈠	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

No.	Examination Item
	verification 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.
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 based on 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 serious deficiencies in its AML/CFT regime.
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

No.	Examination Item
	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 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 Suspicious Transaction Report**" 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 watch list filtering on its wire transfer customers and counterparties based on its established internal rules and operating procedures and saved related records.
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 countries or jurisdictions designated by the

No.	Examination Item
	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 bank account 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 mitigation measures: A correspondent bank should perform customer due diligence (CDD) and enhanced due diligence (EDD) on the respondent bank, and in addition, gather 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.

No.	Examination Item
	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 respondent bank's customers, the monitoring of the correspondent account by the correspondent bank should focus on whether the respondent bank carries out watch list filtering and provides information on originator and beneficiary as required.
(3)	Examination details:
㈠	Determine whether the bank offers cross-border correspondent bank account service; rules and inspection procedures regarding cross-border correspondent bank account do not apply if the business relationship between the bank and other financial institutions is limited to RMA (Relationship Management Application (the process of establishing security keys)).
㈡	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

No.	Examination Item
	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 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 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.

No.	Examination Item
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: 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 mitigation 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, 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

No.	Examination Item
	in person only that online account opening is not allowed (e.g. according to prevailing 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 details:
㈠	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 facilitating ML/TF activities. The related internal control system should require watch list filtering 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.
㈡	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.

No.	Examination Item
	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 watch list filtering 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 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 details 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

No.	Examination Item
	new payment methods to engage in ML/TF activities through fake transactions involving high-price items. New payment technology has aided in the quick cross-border transfer and consolidation of illicit funds.
(2)	Risk mitigation 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 details:
㈠	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 watch list filtering 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.
㈡	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 bank's evaluation of business risk factors (e.g. transaction amount, transaction volume, whether cross-border payment is allowed, etc.).
㈢	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.

刪除:

No.	Examination Item
	whether cross-border payment is allowed) of the bank's e-payment business and the transactions its e-payment customers engage in. Determine whether the bank performs watch list filtering 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.
4	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 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. Based on the examination details 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	

No.	Examination Item
6	
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 mitigation measures: Verify customer identity, perform 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

No.	Examination Item
	by a foreign government or an international anti-money laundering organization.
(3)	Examination details:
㈠	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 intermediaries' use, handling and control of customer data, acceptable certificate of good standing submitted by OBU customers, and conducting watch list filtering 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.
㈡	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 watch list filtering 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

No.	Examination Item
	and whether the bank has been conducting ongoing monitoring of those sampled accounts.
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 and terrorist financing activities. 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 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.

No.	Examination Item
	(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:
㈠	Examine the bank's internal rules and operating procedures for selling insurance products and evaluate whether those rules and procedures 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. 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 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

No.	Examination Item
2	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.

No.	Examination Item
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 (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)

No.	Examination Item
(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 mitigation measures: The bank should establish a sound CDD process to understand fully the 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 mitigation measures.

No.	Examination Item
	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 customers, telltale signs of money laundering, watch list filtering 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 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).

No.	Examination Item
	(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).
(3)	Examination details:
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

No.	Examination Item
	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 transaction. ii Determine whether the bank conducts watch list filtering of transaction related customers and beneficial owners, monitors suspicious transactions, and retains related CDD data.
8	Company
(1)	Risk factors: A corporate organization has 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 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 shell companies: (1) Lacking sufficient information to positively identify beneficial owners or beneficiaries of accounts or other banking activities. (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 respondent bank or the information on the customer's stated business items, or explanation given by the foreign

No.	Examination Item
	respondent 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 shell companies with no apparent legitimate business purpose.
(2)	Risk mitigation measures: The bank should establish internal rules and operating procedures for identifying the account risks of corporate customers. The bank should assess the ML/TF risks of corporate customers and carry out ongoing account and transaction monitoring on the basis of risk.
(3)	Examination details:
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 corporate customers.
②	Confirm the additional CDD measures taken by the bank for 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 corporate customers and reporting suspicious money laundering transactions (identification by system or

No.	Examination Item
	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 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 (PEP)
(1)	Risk factors: 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 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. 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

No.	Examination Item
	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 mitigation 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 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 system, customer's declaration (however customer's declaration does not relieve the bank of its responsibility),

No.	Examination Item
	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.
(3)	Examination details:
㈠	Whether the bank determines the 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.
㈡	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.
㈢	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.
B	**Customer due diligence (CDD)**
(A)	Measures for verifying customer identity
1	Examine whether the bank's internal rules and operating procedures include: ㈠ Not accepting or maintaining business relationship with anonymous accounts or accounts in fictitious names. ㈡ Setting the time for conducting CDD. ㈢ Obtaining information for CDD (including information on customer, its agent, beneficial owner or senior management) and adopting risk-based approach to identity verification (including verification methods and procedure for

No.	Examination Item
	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). 5 Carrying out watch list filtering on existing customers (including the customer, its agent, beneficial owner or senior management) who apply for a new account. 6 When the bank relies on a third party to perform CDD on the customer, its agent, beneficial owner or the purpose and nature of business relationship, 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. 8 Conducting 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 customer's account is operated, which is not consistent with the customer's business profile.
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 operation in its internal audit system and employee training program.
4	Evaluate whether the bank readily updates the sanction list and list of high risk countries or jurisdictions in its database (including but not limited to countries or

No.	Examination Item
	regions with serious deficiencies in their AML/CFT regime, and other countries published by international organizations on AML/CFT or countries or regions that do not or insufficiently comply with the recommendations of international organizations on AML/CFT as forwarded by the FSC), and based on which, perform watch list filtering on new customers.
5	When necessary, the examiner can conduct verification according to the following procedure: ㈠ Select, 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. general 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 for which there is a suspicion 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. ㈡ 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 watch list filtering on customers (including customer, its agent, beneficial owner or senior management). ㈢ Evaluate whether the bank's criteria for allowing accounts opened with exceptions affect the effectiveness of its CDD. ㈣ Screen occasional transactions carried out by customers without a bank

No.	Examination Item
	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 and beneficiaries. 5 Examine 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 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 Examine whether the bank's internal rules and operating procedures include:
1	㈠ 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)). ㈡ 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,

No.	Examination Item
	organization or trustee, and verification methods. 3 Watch list filtering to be performed on customers (including customer, its agent, beneficial owner or senior management) who apply for a new account. 4 When the bank relies on a third party to perform CDD on the customer, its agent, beneficial owner or the purpose and nature of business relationship, does the bank audit and monitor the third party's use, processing and control of customer information? 5 Internal rules and operating procedures for immediately filing suspicious ML/TF transaction report at the time a customer opens an account. 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.
2	
(C)	Watch list filtering
1	Whether the bank's board of directors or senior management oversees the establishment of internal rules and operating procedures for risk-based watch list filtering, which specify who should be subject to filtering, matching and filtering logic, implementation procedure for the filtering operation and evaluation standards.
2	Does the bank use a risk-based approach to determine who should be subject to

No.	Examination Item
	watch list filtering procedure; those people should 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 filtered 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 filtering should also cover the PEP's beneficial owner, family members and close associates.
3	Whether the bank specifies in its internal rules and operating procedures the test frequency, test items and methods for its watch list filtering 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 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.
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 rules and operating procedures for watch list filtering the logic for matching and screening customer data, relevant

No.	Examination Item
	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 filtering based on Romanization is 100% match or only the sequence of 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 identified 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; and 3) adopt risk mitigation 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**").
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: ㈠ Spot check high-risk new accounts (for any business) to examine whether the bank has conducted watch list filtering on the customer and related parties before completing the account opening and retained relevant inquiry data. ㈡ Spot check transactions that do not involve the account (including credit card

No.	Examination Item
	and "walk-in" customers) to examine whether the bank has the incidence of conducting watch list filtering after the transaction is completed, whether the bank saves filtering data, and whether the filtering logic is consistent with the bank's internal rules. 3 Examine 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 watch list filtering 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. 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 watch list filtering 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

No.	Examination Item
	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.
2	Whether the bank has established internal rules and operating 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.
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 high-risk customers, is the bank's frequency of risk reassessment for customers at other risk levels commensurate with the

No.	Examination Item
	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 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.
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.
(F)	Political exposed persons (PEP)
	(With regard to "**Risk factors**", "**Risk mitigation measures" and "Examination details), refer to "Politically exposed persons"** under the section "**Effectiveness of internal controls**" of "**Policies and Procedures**").
(G)	Decline to establish business relationship with customer
1	Whether the bank has established internal rules and operating procedures for declining to establish business relationship with certain customers.
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.
C	**Ongoing monitoring and suspicious transaction report (STR)**
(A)	Whether the bank has selected or developed suitable red flags based on its size of assets, geographic locations, business profile, customer base profile,

No.	Examination Item
	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.
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 spot check the CDD and EDD data of high-risk customers to determine whether information that aids in the analysis of ML/TF risks has been completely posted or captured in the information system.
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

No.	Examination Item
	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). 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 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.
4 (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 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

No.	Examination Item
	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.
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 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.
3	For suspicious ML/TF transaction cases under investigation named in the correspondence from a law enforcement agency, the bank should have internal

No.	Examination Item
	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 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.
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

No.	Examination Item
	performed by the head office if the design of ongoing monitoring mechanism throughout the bank is 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 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.

No.	Examination Item
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 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 assessment,

No.	Examination Item
	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 details under the section "Watch list filtering".
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 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.
6	Whether a bank files a STR or not is partly predicated on the subjective judgment

No.	Examination Item
	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 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.
(D)	Whether the bank files cash transaction reports (CTR) according to rules.
1	The examiner should spot 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, spot check control weakness, and confirm the manner by which the bank outputs reportable large cash transaction data.
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, such as department

No.	Examination Item
3	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. If the bank relies on system output of all large cash transactions and then manually picks reportable transactions, the examiner should spot 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 accuracy of manual pick operation.
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.
D	**Risk prevention program (risk assessment)**
(A)	Whether the bank sets specific risk assessment items based on the identified risks. Specific risk assessment items should cover at a minimum customers, geographic locations, products and services, transactions or delivery channels.
1	Refer to Appendix A with regard to a risk assessment methodology. However the

No.	Examination Item
	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 for high-risk products, services, transaction channels, customers or geographic locations identified), customer risk levels and classification rules, overall risk tolerance, and improvement mechanism when tolerance is exceeded, and those documents are passed by the bank's board of directors.
3	Whether risk assessment items cover completely the aspects of geographic locations, customers, products and services, transactions or delivery channels (referred to as "inherent risks" below).
4	Whether the bank includes appropriately internal and external information into factors to be considered in its ML/TF risk assessment and save relevant information, which should include but is not limited to: communication with relevant business units, country risk assessment result (e.g. identified high-risk lines of business), sanctioned jurisdictions or sanction lists released by international organizations or foreign governments, and red flags for suspicious money laundering activities.
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 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

No.	Examination Item
	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.
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)	Whether the bank has established risk management measures corresponding to its risk profile to reduce the identified risks.
1	Are specific documented risk mitigation measures established for inherent risk items that pose higher risk based on the assessment result?
2	Below are a few examples of enhanced due diligence (EDD) measures for high-risk customers. However the bank may decide the extent of applying EDD using a risk-based approach and establish standard operating procedures: ㈠ Verification of customer identity: Names or aliases once used by individual customers; obtain replies to correspondences sent the address provided by customers and signed by individual customer/authorized signatory of legal persons or organizations or conduct phone interview; obtain supporting data evidencing the sources of customer wealth and funds (sources of funds refer to the original sources that generate such funds, e.g. salary, investment proceeds, disposal of real estate, etc.); understand the latest financial status of customer who is a legal person, organization or trustee and analyze its business activities

No.	Examination Item
	and business dealings (e.g. whether there are frequent cross-border transactions), and establish a datafile on such customer's assets, sources of funds, flow of funds, and currency and amount of its main business activities (examples of supporting data on sources and flow of funds include list of major suppliers, list of major customers and major trading areas); if the customer is a legal person, understand its beneficial owners; conduct onsite visits to confirm the actual operations of a customer; and obtain information from banks the customer used to work with and inform such banks. 2 Relevant data on the purpose of the account and the purpose of transaction: Anticipated account activities (e.g. anticipated transaction amounts, purposes and frequency). 3 Approval mechanism before establishing or entering a new business relationship: Obtain the consent of senior management with approval authority set up based on internal risk considerations. 4 Increase the frequency of customer due diligence. 5 Ongoing review: Conduct enhanced ongoing monitoring of business relationship.
3	For PEPs and their family members and close associates, whether the bank determines customer risk level according to rules or based on risk.
(C)	Production of risk assessment report
1	Whether the bank generates a risk assessment report and submits the report to the FSC for reference.
2	Time 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 number of high-risk customers open or close an account or the bank undergoes merger and acquisition (that is, when there is

No.	Examination Item
	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 rules and operating procedures.
3	The bank's internal rules and operating procedures should describe specifically the frequency of 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, use one single indicator as the decisive factor for assigning high or low ML/TF risk; is full consideration given to qualitative and quantitative factors; is the same risk level assigned to businesses or products with higher inherent risk (correspondent account, foreign exchange transaction, 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 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 examination, the bank should then propose an appropriate

No.	Examination Item
	improvement plan.
8	Are all control effectiveness factors considered actually included in the internal control procedures; the examiner should spot 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?
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?
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 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.

No.	Examination Item
2	When an employee has any of the following situations, the bank should spot check the works handled by the employee, and if necessary, ask its audit unit to assist in investigation: ㈠ The employee exhibits a lavish lifestyle that cannot be supported by his or her salary. ㈡ The employee is reluctant to take a scheduled vacation without a reason. ㈢ 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.
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.
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.

No.	Examination Item
(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 compliance unit handles businesses other than AML/CFT.
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.
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.
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 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

No.	Examination Item
	laundering transactions, is the division of labor for related investigation works clearly specified? The examiner should also spot check whether the actual operation is consistent with the contents of relevant internal rules and operating procedures.
5	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.
6	Whether the chief AML/CFT officer, AML/CFT compliance unit personnel and AML/CFT supervisor of domestic business units meet the qualification requirements.
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.
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?
(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 operating procedures for information sharing within the group on condition that the regulatory requirements on data

No.	Examination Item
	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.
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 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

No.	Examination Item
	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 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 facilitate monitoring and controlling unusual transactions within the group.

No.	Examination Item
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 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

No.	Examination Item
	branches and subsidiaries apply the same criteria as the head office.
(D)	AML/CFT program effectiveness audit (independent testing)
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. 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.
2	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:
3	① The 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. ② Audit whether the bank's ML/TF risk assessment result is reasonable based on the bank's risk profile (customer, product, service, geographic location, etc.). ③ Conduct 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

No.	Examination Item
	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 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. 2. Determine whether the filtering or screening indicators set by the bank are reasonable and cover all self-identified higher-risk products, services, customers or geographies. 3. Determine 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. 4. Determine 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

No.	Examination Item
	internal audit unit covers all bank business units (including overseas branches and subsidiaries) and whether the depth of audit is planned based on risk. ㈡ Whether 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. ㈢ 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: ㈠ Higher-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 ㈡ Select 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 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.