[Provisional Translation]

The original texts of the FAQs are prepared in Japanese, and this translation is only provisional. The translation is to be used solely as reference material to aid the understanding of the FAQs and is subject to any future changes.

Frequently Asked Questions Regarding "Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism"

March 31, 2026

Strategy Development and Management Bureau
Financial Services Agency

Definition

- ✓ Money Laundering and Terrorist Financing

  The term "money laundering" refers to the attempt to evade detection and confiscation of proceeds obtained through criminal activity, including but not limited to proceeds obtained by reselling assets acquired through criminal acts, by concealing the source and ownership of the proceeds.

  The term "terrorist financing" refers to the procurement, transfer, storage, or use of funds, etc., for the purpose of funding the execution of terrorist activities or funding the activities of terrorist organizations.

  In this FAQ, “Money Laundering” is referred to as "ML," and "Money Laundering and Terrorist Financing" is referred to as "ML/FT."

- ✓ The Anti-Money Laundering/Countering the Financing of Terrorism Guidelines

  The Guidelines set out and clarify what the Financial Services Agency (FSA) requires financial institutions to do, i.e. “Required Actions for a Financial Institution.” These requirements are reviewed during FSA’s monitoring processes of financial institutions, and the FSA serves to define future monitoring schemes.

  In this FAQ, the term “Anti-Money Laundering/Countering the Financing of Terrorism Guidelines is referred to as "the AML/CFT Guidelines.”

- ✓ Act on Prevention of Transfer of Criminal Proceeds

  In this FAQ, the “Act on Prevention of Transfer of Criminal Proceeds” is referred to as "APTCP."

- ✓ Financial Action Task Force (FATF)

  FATF is an intergovernmental panel mandated in 1989 as part of the Economic Declaration of the Arch Summit. Delegations from each member jurisdictions analyzes the typologies of ML/FT, develop and continuously strengthen international standards (FATF 40 recommendations/interpretive notes) for combating money laundering and terrorist financing, and perform reciprocal evaluation of each member jurisdictions for their implementation (mutual evaluation).

In the FAQ, the term "FATF" is used.

✓ National Risk Assessment and Its Follow-up Report (NRA-FUR)

The National Public Safety Commission (“NPSC”), which collects, categorizes, and analyzes information on the transfer of proceeds of crime and suspicious transactions, shall obtain information from the administrative agency supervising the specified business operator, on the characteristics of products and services handled by them and the status of countermeasures against money laundering, etc., and shall prepare and publish the NRA by utilizing their intelligence and expertise.

In the FAQ, "NRA" or “NRA-FUR” is used.

✓ Transaction filtering

The filtering process is used by financial institutions to detect, prevent, and manage transactions that violate laws and regulations, such as the removal of anti-social forces and sanctioned persons or entities. The term "transaction filtering" in these Guidelines and the FAQ refers to a method of reducing risk by preventing transactions by antisocial forces and sanctioned persons or entities, etc., through screening against sanctions lists prior to transactions or when such lists are updated. The concept is used to include so-called name screening.

The term "name screening" refers to checking whether the names of new or existing customers fall under the sanctioned list to be checked. Guidelines, II-2 (3)(ii) CDD【Required actions for a financial institution: 4 and 5】 correspond to this.

✓ Correspondent relationships/ Correspondent banking/ Correspondent counterparty

The term "Correspondent relationships" is used as a concept including the following relationships:

① Nostro account (our account, an account held in a foreign currency to settle foreign currency funds through interbank transactions)

② Vostro account (the counterparty's account; an account held in a foreign currency by the counterparty's bank in order to settle foreign currency

funds through interbank transactions)

③ RMAs (an application exchanged for communication in SWIFT Relationship Management Application) and establishes relations that allow the exchange of messages especially instructions on fund transfers and the establishment of letters of credit, on the SWIFT network.

- ✓ Director in charge of AML/CFT
  - ✓ PerIII-2, "involvement of management and Understanding" 【Required actions for a financial institution: ii】 of the AML/CFT Guidelines, Director in charge of AML/CFT means an officer who has been appointed as a "person responsible for AML/CFT."

I-1 General Concepts on "Risk-based approach"

To this end, **management** of financial institutions needs to take the lead in establishing cross-regional and cross-departmental governance, and under this governance, related departments need to continue their efforts to continuously improve AML/CFT measures, in order to ensure that these measures against money laundering and terrorist financing function effectively in the sales divisions, which are the actual points of contact with customers.

【Q】

What is the definition of "management" in this the AML/CFT Guidelines?

【A】

"Management" in this AML/CFT Guidelines is a concept that may include executives who are responsible for AML/CFT, including risk-management, systems-investment, and administration, as well as executives who are responsible for the relevant front office department and internal audit department, in addition to the executives who have legal representation. The scope of the management team and its roles and responsibilities should be thoroughly discussed and examined by each FI and other stakeholders under the leadership of the senior management.

The breakdown of "management" as defined in the AML/CFT Guidelines and the division of responsibilities should be clarified in documents such as internal procedures.

I-2 Measures required of financial institutions

(2) Involvement and understanding of management

In establishing the aforementioned control framework, **it is essential for the management to be involved in countermeasures such as taking the initiative in establishing governance for control**, rather than leaving it to the relevant departments to deal with the risk, based on the understanding that the risk of money laundering and terrorist financing can be a serious business risk.

【Q】

What is the way in which the management takes the initiative in establishing governance for control?

【A】

With respect to the involvement of the management team, the Board of Directors should recognize that the risk of money laundering and terrorist financing may become a serious business risk, and position measures against money laundering and terrorist financing as one of the important issues in the management strategy, or establish a cross-organizational framework under the responsibility of the management, and implement strategic measures such as securing human resources, training, and resource allocation

As evidence that the Board of Directors, etc. regards anti-money laundering/terrorist financing measures as one of the important issues in its management strategy, etc., evidences such as the minutes of the Board of Directors, etc. containing the contents of reports, instructions and comments from the management, disclosure reports and annual reports stating that the Board of Directors, etc. recognizes the risk of money laundering/terrorist financing as a management issue and takes appropriate measures according to the risk, may be considered.

I-3 Roles of industry associations and central institutions

In cases in which a central institution conducts transactions for the customers of its member financial institutions via outsourcing or agency relationships, or in cases in which an internationally operating bank is relied upon by other banks to undertake their customers' foreign remittances, **such a central institution or internationally-operating financial institution is also required to establish the necessary and adequate control framework to undertake AML/CFT in accordance with the risk-based approach**.

【Q】

With regards to the statement that "such a central institution or internationally-operating financial institution is also required to establish the necessary and adequate control framework to undertake AML/CFT in accordance with the risk-based approach", when an FI acts as an intermediary or an agent for another FI, what are the expected AML/CFT countermeasures? The point of contact with the end client is at the FI outsourcing its business and can the intermediary/agent FI employ lighter countermeasures in light of the presence of a FI conducting the initial AML/CFT measures? It can also be argued that such FI is outsourcing some processes due to lack of cross border payments or lack of knowledge and shall the intermediary/agent FI implement enhanced AML/CFT measures than ones conducted against its own clients?

【A】

The primary responsibility for confirming the remittance originator and beneficiary, the purpose of remittance, and risk-based confirmation procedures at the time of acceptance of fund transfer requests is expected to be carried out by the outsourcing FI. When considering the content of such confirmation procedures, FIs should examine their own risk control framework for ML/FT in terms of whether or not they can effectively manage the risk to keep it within their risk appetite.

In addition, the intermediary/agent FIs should have an appropriate understanding of the control framework of the outsourcing FI, and should have a mechanism in place to obtain necessary information to manage its own ML/FT risks. If necessary, additional inquiries should be made into the customers of the outsourcing financial institutions that are not their own customers, and other risk-based measures such as monitoring and filtering of transactions, reporting of suspicious transactions, and record keeping should be taken.

I-4 Purpose of the FAQ and Supervisory actions

Keeping Japan's financial system sound and immune from ML/FT is extremely important, and as the financial regulator, the FSA properly conducts monitoring of financial institutions' measures and progress in developing AML/CFT in accordance with the Guidelines.

If such monitoring and other measures identify **problems with a financial institution's ML/FT risk management, including an inadequate implementation of the Required actions in the Guidelines (Refer to Q1)**, the FSA makes financial institutions improve by taking necessary administrative actions prescribed in relevant laws such as reporting orders and business improvement orders, referring also to Supervisory Guidelines that are stipulated for each industry type.

【Q1】

In cases where inadequate measures at an FI were identified concerning "Required actions for a financial institution", the Guideline states that an administrative action will be taken. Will the FSA impose an administrative action to an FI even if the FI does not commit make legal violations?

【A】

Administrative actions are conducted in accordance with laws and regulations stipulated for each business category.

AML/CFT Guidelines' "Required actions for a financial institution" clarifies the expectations in ML/FT risk management in light of the purpose of the relevant laws and regulations, and if ML/FT risk management is deemed to be inadequate, FSA may take administrative actions against the FI in accordance with the laws and regulations.

II-1 Objectives and Implications of Risk-based Approach

The risk-based approach in combating money laundering and terrorist financing means that financial institutions, etc. identify and assess their own inherent risks of money laundering and terrorist financing, and take risk mitigation measures in order to effectively reduce such risks to **within their risk appetite**.

【Q】

In terms of AML/CFT, RBA is defined as "within their risk appetite". What does this concept practically mean? How can we specifically consider this as "within their risk appetite"?

【A】

FI's risk appetite means that ML/FT risk identified and assessed by themselves should be within the scopes acceptable to the FI's risk management capability.

The expectation is that evidence of current risk being within the risk appetite threshold be approved by the senior management in charge of AML/CFT and then documented.

II-2 Identification, assessment, and mitigation of risk

II-2 (1) Risk identification

(Main paragraph)

In order to conduct a comprehensive and specific verification of risk that an entity faces, it is necessary to consolidate internal information and conduct analysis from a company-wide perspective. Therefore, it is necessary for the management to take the initiative in ensuring cooperation and collaboration among all related departments, rather than leaving it to the department in charge of countermeasures against money laundering and terrorist financing.

When undertaking such evaluation, financial institutions must appropriately consider the NRA and the analyses conducted by foreign authorities and industry associations. Based on these considerations, it is important to take into account **both the analyses commonly applicable to every sector and those specific to a certain sector, capturing both characteristics**.

【Q】

Please provide specific examples of both the analyses that each sector should refer to and the analyses by sector according to the characteristics of each sector.

【A】

"Analysis that should be commonly referred to by individual sector" are those that should be referred to analysis, such as NRAs or FATF published guidance on RBA. "Analysis by sector" refers to the sectoral guidance provided by FATF (banks, crypto-assets, etc.), as well as the analysis published by international organizations and foreign authorities, and the collection of case studies shared and published by Industry Association for members.

II-2 (1) Risk identification

【Required actions for a financial institution: i】
Identify the ML/FT risks it faces by **comprehensively and specifically evaluating risks (Q2)** of the products and services offered, transactions types, the countries and geographic areas of transactions, customer attributes, and other relevant factors, while **considering the results of the national risk assessment (Q1)**.

【Q1】

What is the specifically expected for risk identification upon review of, but not limited to, national risk assessment?

【A】

In addition to the risk items that can be read from the NRA, FIs need to comprehensively identify the products/services provided by FIs., transaction types, the countries/regions involved in direct/indirect transactions, and customer attributes by referring to the AML/CFT Guidelines and this FAQ, and then verify them in order to identify specific risk items in line with actual practices.

It is useful to identify ML/FT risk by referring to materials that are considered useful for identifying FI's own risks (e.g., guidance on RBA published by FATF) in order to develop a risk control framework. Therefore, in addition to NRA and the AML/CFT Guidelines, additional materials could be used as reference.

【Q2】

How can we conduct a comprehensive and specific evaluation of risks?

【A】

Methods of "Identify(ing) the ML/FT risks it faces by comprehensively and specifically evaluating risks" may differ depending on the individual FIs. FIs should comprehensively identify the products/services they offer based on transaction types, countries/regions involved in transactions, and customer attributes. The identified risk shall be clear so that it can be used to analyze potential risk factors in the FI's business as usual, rather than making vague and simplified conclusions

For example, FIs need to identify risk based on each product and service offered by themselves, such as "ordinary deposits" "term deposits", "US dollar ordinary deposits" and "EUR term deposits". Similarly, the attributes of each country/region or customer involved in all transaction types and transactions used by customer need to be examined at the same level as above to identify the risks.

In conducting this verification process, it is necessary to appropriately take into account the findings of NRA, foreign authorities and Industry Association, etc. In addition, it is necessary to take into account the characteristics of ML/FT risk that the FI faces, including analyses of STR

【Q3】

For example, if a FI provides services to a provider of a product or service that the NRA listed in the "Risk of Products and Services", what are the points for consideration when "comprehensively and specifically" "evaluating" the risks that FI faces?

【A】

With respect to the identification and evaluation of risk as a customer attribute of a person who provides a product or service listed in the "Risk of Products and Services" in the NRA, instead of uniformly determining that it is high risk only because it provides products and services described in the NRA, it is necessary to identify and evaluate risks by taking into account the descriptions of "risk factors" and "Measures to Mitigate Risks" among the descriptions of "Risk of Products and Services" in the NRA, as well as actual customer transactions and other factors.

In addition, when conducting a customer risk assessment for such service providers as customers, it is necessary to take into account the business model and actual transactions of such customers.

II-2 (1) Risk identification

【Required actions for a financial institution: ii】

When conducting a comprehensive and specific evaluation, **taking into account the financial institution's specific features such as the geographic attributes of its business area, business environment**, and management strategy, etc.

【Q】

In conducting comprehensive and concrete evaluation, "taking into account the financial institution's specific features such as the geographic attributes of its business area, business environment" and "management strategy" is required. What is specifically required?

【A】

"The geographic attributes of its business area" refers to the characteristics of the geographical elements of the region. For example, if FIs' business operation covers an international trade-intensive area, if the FI have active anti-social force activities in the area, if there is a headquarter of anti-social forces in the area, the FI may need to take into account the unique characteristics associated with risks related to the region. When conducting the analysis, for instance, if the FI operates in a region where trade activity is common, the likelihood of handling foreign trade or products including seafood will be higher. Under these circumstances, FIs are required to comprehensively identify the associated risk from the geographic aspect; this includes analysis of products dealt by a customer and obtaining information on exporter/importer for the purpose of complying with economic sanctions. In terms of the "business environment", it is necessary to consider factors related to FIs own business, such as regulatory conditions related to ML/FT and competitors' AML/CFT measures, and to examine the risks. . For example, when competitors enter the market (basically when their own competitors enter the market), the entry of new competitors may change inherent risks of ML/FT due to intensified competition, changes in services, and transaction volumes change. Therefore, for example, if the entry of new competitors impacts risks related to ML/FT of the market as a whole, FIs need to identify at the earliest possible stage whether there are any new risk items to be analyzed, rather than waiting for periodic revisions to risk assessment sheet scheduled once a year. When a customer conducts cross-border transaction, it is required to conduct customer risk assessment including ML/FT risk assessment of the country/region of the counterparty.

The "management strategy" may include various action plans such as doubling revenues, obtaining new customers, acquiring overseas financial institutions.

With regard to the matters that the company has set as priority areas in its management strategy, it is necessary to verify in what ways the products and services provided by the institution could be used for ML/FT if the company proceeds the strategy.

It would be desirable to understand the magnitude and change in significant risks for the financial institution in a timely and appropriate manner, by identifying and quantitatively analyzing key indicators to understand the risks of its products and services, transaction types, countries and geographic areas, customer attributes, and other relevant factors in light of the complexity of its business environment and the business strategy. These major indicators related to the identification and assessment of risks likely include the number of cross border remittance transactions, the number of internet banking transactions, the number of non-resident transactions, the number of suspicious transaction reports, and the number of frozen accounts by external request. The quantitative analyses using specific indicators are determined by each financial institution based on the business environment, management strategy, risk profile, etc. of the respective financial institution.

II-2 (1) Risk identification

【Required actions for a financial institution: iii】

When evaluating the countries and geographic areas of transactions, comprehensively evaluate the possibility of direct and indirect transaction relationship, including the high-risk countries and geographic areas designated by the FATF and domestic and foreign authorities, **and understand the risks**.

【Q1】

The Guidelines state that "When evaluating the countries and geographic areas of transactions, comprehensively evaluate the possibility of direct and indirect transaction relationship, including the high-risk countries and geographic areas designated by the FATF and domestic and foreign authorities, and understand the risks." What are the implications of an indirect transaction?

【A】

In some cases, transactions are conducted with neighboring countries or regions, such as jurisdictions subject to sanctions, or transactions conducted by customers are conducted in high-risk countries or regions, such as countries or regions subject to sanctions. In other cases, transactions with ML/FT high risk county are conducted, through ML/FT low risk countries.

In addition, even if a customer is located in Japan, if the customer establishes subsidiaries/joint ventures in countries and regions surrounding high-risk countries, such as those subject to sanctions, there is a possibility that the funds will flow out to countries subject to economic sanctions through the subsidiaries/joint ventures.

Regarding this ML/FT risk, FIs should understand not only the customer's commercial flow but also the actual status of the subsidiaries and joint ventures of the customer, and, if necessary, the actual status of their counterparties as part of their risk assessment Furthermore, FIs are required to fully understand whether the customer is aware of the actual status of these subsidiaries, etc. and whether the customer has a check-and-balance function over the subsidiaries, etc.

For subsidiaries and joint ventures located in areas neighboring high risk jurisdictions, it is important to conduct the aforementioned checks, in addition to checks on counterparty and products. It is up to each FI, however, in deciding on the scope of entities to be investigated and method of investigation, taking into account the risk faced by the FI.

Such evaluation must be conducted to entities where the FI extends loans but even for

other entities, based on information from various sources, if they are deemed to be operating globally, such evaluation must be conducted. These include, but depending on circumstances, checking for existence of subsidiaries or joint ventures located near sanctioned countries or jurisdictions and their potential transactions with sanctioned entities or persons.

【Q2】

For example, if an FI is primarily engaged with an international trade business operator, does it need to evaluate ML/FT risk of the country where their customers are located?

【A】

For the purpose of customer risk assessment, if the client is engaged in an activity related to transactions with foreign countries or running businesses abroad, it should be important to understand the country and region-specific ML/FT risks the client is exposed to.

II-2 (1) Risk identification

【Required actions for a financial institution: iv】

When offering new products and services, or conducting transactions using new technologies /those with new characteristics, **prior to launch of transactions (Q2), evaluate the risks associated with such products and services, including the effectiveness of the risk control framework of alliance/business partner, outsourcing contractor, and target company in M&A or the acquired company involved in the provision of such products and services (Q1).**

【Q1】

What matters should be kept in mind when FIs evaluate the effectiveness of the risk control framework of their alliance/business partner, outsourcing contractor, and target company in M&A or the acquired company

【A】

FIs are obligated to develop a risk-based control framework based on their risk assessment to ensure that their businesses and services are not used to facilitate ML/FT. From the perspective of its impact on the products and services it provides, FIs are required to evaluate ML/FT risk as part of its risk-based management, including the effectiveness of the risk control framework of its alliance/business partner, outsourcing contractor, and target company in M&A or the acquired company ("related entities, etc.") from the FI's products and services point of view.

【Q2】

What matters should be kept in mind about evaluating ML/FT risk prior to providing the relevant products and services.

【A】

In addition to introducing new products and services, events such as acquiring domestic or foreign companies or engaging in a partnership agreement may create similar situation. FIs will face different risks under such circumstances and the first line and the second line must cooperate and conduct an ML/FT risk identification and analysis prior to the launch.

Conceivable scenario to the above, for example, is when an FI is considering offering a deposit-only type of dummy account (so-called virtual account) linked to a corporate account to its customers as an account receivable service. The risk of ML/TF should be examined considering factors including the purpose of use of the virtual account by the

prospective entity using the virtual account.

In cases where customers in fact transfer third-parties' funds via virtual accounts, it is considered necessary to take risk mitigation measures based on such usage.

Another expected scenario is that when an FI introduces new products and services relying upon other partner corporations' customer verification processes, it is essential to confirm the effectiveness of their ML/FT risk control framework. It is also essential to verify those partner stakeholders are neither anti-social forces nor sanctioned persons by checking their related parties and beneficial owner.

In addition to above, it is also essential to identify the ML/FT risks that FI's business partners face and how they manage them; the FIs would need to continuously monitor them.

Furthermore, if a risk changes due to a change in the nature of the products and services after the service and/or product is launched, it is necessary to review the risks again and implement corresponding mitigation measures.

It is a matter of fact but in an event that the services provided in cooperation with the relevant partner fall under the category of specified business (APTCP Appendix Table and Article 6 of the Enforcement Order of the APTCP), the FI shall prepare and retain transaction records and file suspicious transaction reports in the event of transactions pertaining to the specified business. In addition, the FI is required to carry out the development of a control framework in order to properly retain transaction records and implement suspicious transaction reporting measures (see Article 11 of APTCP and items of paragraph 1 of Article 32 of the Ordinance for Enforcement of APTCP).

II-2 (1) Risk identification

【Required actions for a financial institution: v】
Conduct comprehensive and specific evaluation of ML/FT risks with management taking the lead in ensuring coordination and collaboration among all relevant departments

【Q】

With regards to "Conduct comprehensive and specific evaluation of ML/FT risks with management taking the lead", what specific actions are requested from the board and senior management?

【A】

For ML/FT risk identification, the necessary responses to be taken by the board and senior management are: 1. ensuring a framework for identifying ML/FT risk through organizational collaboration; 2. coordinating the interests of each department at the management level; 3. providing guidance and support for the smooth and effective identification of ML/FT risks; and 4. taking the initiative in making decisions on the allocation of resources that enable them.

【Q2】

What matters should be kept in mind about the method of coordination and collaboration between the first and the second lines in a comprehensive and concrete evaluation to identify risks?

【A】

Since the first line has the most information on customers' customers, customers' trade flows, and the actual status of products and services, it is necessary to utilize the information collected by the first line in order to identify associated risks.

In identifying risks, the second line may organize the information necessary for risk identification, such as the nature of the products and services and the customer attributes (e.g. non-face-to-face transaction risks, whether transactions with foreign countries are expected, whether cash is accepted or not, wealth accumulative nature, whether high-risk customers are expected to use the products and services), and then the first line may examine if these characteristics are applicable for each product and services and customers, and then return the information to the second line. On the other hand, the first line may provide information on its own products and services and the customer attributes after organizing such information.

The basis of this lies in the fact that the second line is required to provide with the first line the appropriate training on how to identify ML/TF risks in line with the products and services, transaction types, countries/regions, and customer attributes. At the same time, it is necessary for the first line's understanding of risk-based ML/TF risk management methods, including risk identification.

II-2 Identification, assessment, and mitigation of risk

(2) Risk assessment

【Required actions for a financial institution: i】

Establish an enterprise-wide policy and specific methods for its risk assessment, and **conduct assessments of the ML/FT risks identified (Q1), (Q2)** in "(1) Risk Identification" based on concrete and objective evidence in accordance with the said policy and methods.

【Required actions for a financial institution: iv】

Document the results of the risk assessment (Q1), and utilize them for developing measures necessary for risk mitigation.

【Q1】

When in "conducting assessments based on concrete and objective evidence" and "documenting the results of risk assessment", what are the factors that need to be taken into account?

【A】

When conducting an evaluation based on specific and objective evidences, FIs may evaluate based on specific and objective analysis and evaluation of actual transactions, customer attributes, and suspicious transaction reports filed and its trends, and the damage and typologies of financial crime.

For example, FIs need to base their assessment on the volume/value of transactions, the rate of occurrence of events, and the degree of impact arising from such events, as well as its own business environment, management strategy, and risk profile.

"Rate of occurrence" refers to the likelihood of incurring tangible and intangible losses. In addition, "degree of impact" refers to the size (large/small) of expected tangible and intangible losses, etc. Examples of "tangible and intangible losses" may include administrative order and sanctions imposed by domestic and foreign authorities, the elimination of correspondent relationships, and reputational risks.

We believe that FIs need to document in advance how to consider the above factors and how to evaluate them.

Risk assessment conducted by the government such as the NRA ones conducted by industry associations, and FATF's (Note), may be used to assess consistency in the perception of risks for the industries and countries included in these assessments.

In addition, the results of risk assessment need to be documented based on the above

analyses, and "documenting the results of risk assessment" means the task of such documentation. In the process of documenting risk assessment outcome, it is necessary to describe the risk mitigation measure being implemented (detailed measures based on risk assessment findings for each category, etc.), as well as the contents and assessments of the effectiveness evaluations conducted from time to time or periodically.

When the products and services it offers, transaction types, countries and geographic areas of transactions, customer attributes, etc., are wide-ranging, it would be desirable for each FI to break down the associated risks into smaller categories and assess the risks for each category. Then the assessment results could be consolidated to create a firm-wide risk assessment report, and the results of the firm-wide risk assessment are visualized in a risk map and reviewed in a timely manner to promote firm-wide understanding and implementation for the board and business department.

(Note)Methodology, Recommendations, Interpretive Notes, Sector Guidance/Guidance, High-Risk Jurisdictions subject to a Call for Action, Jurisdictions under Increased Monitoring are published by the FATF, and information related economic sanctions imposed by domestic and foreign authorities

【Q2】

What are some specific points to note about how to collaborate with sales departments for risk assessment?

【A】

Risk assessment requires an accurate understanding of ML/FT risk by FIs and others. Therefore, only the second line, which acts as the main control function, working to assess the risks should be avoided so that the results will not be unrealistic. Specifically, the first and the second line need to work closely together so that the first line, having the most information on customers, products, and services, can provide inputs to the second line. The first line, during the course of its business, have maintained strong relationship with clients and obtained information such as counterparties of clients, business flow, products /services, and channels and these can be incorporated to the risk assessment for a more holistic assessment.

The compliance related department (the second line) needs to establish company-wide policies and specific methods for risk assessment so that the sales department (the first line) can clearly understand the circumstances to consider when implementing a risk assessment.

In addition, the compliance related department (the second line) needs to conduct a

final risk assessment based on risk assessment conducted by the sales department (the first line), while taking into account the results of the analysis of suspicious transaction reports and other factors.

Besides, as a prerequisite for such collaboration between the first line and the second line, the second line should provide appropriate training to the employees belonging to the first line on how to assess ML/FT risk in accordance with products/services, transaction types, countries/geographic areas, and customer attributes to ensure that they have sufficient understanding of the risk-based ML/FT risk control methodology including risk assessment.

II-2 (2) Risk assessment

【Required actions for a financial institution: ii】

In making the assessment in (1) above, consideration should be given to the analysis of **the status of Suspicious Transaction Reporting, etc. (Q1)**

【Required actions for a financial institution: iii】

Analyze the status of suspicious transaction reported (Q2), for example, quantitative information such as the number of reporting should be analyzed by division, location, reporting factors, detection scenario, etc., and utilized for risk assessment.

【Q1】

What is the "etc." in "the status of Suspicious Transaction Reporting, etc." specifically?

【A】

For example, in addition to analyzing the status of fraudulent use of one's own account and the records of external inquiries from investigative authorities, in cases where financial crimes such as special fraud have occurred, asset freezing requests from police, reporting from customers, and publicly known information such as news reports on customer, etc., can be used to assess risks.

【Q2】

How are submitted STR required to be analyzed? Also, how should the analysis be carried out when the number of reporting is limited?

【A】

In addition to reviewing customer risk assessment for the customer whose transaction triggered an STR, the suspicious transaction should be analyzed by focusing on factors such as products/services, transaction types, country/geography, customer attributes, reasons for reporting/detection. These information then shall be used for the FI's identification of risks, assessment, risk mitigation measure, and review of customer risk assessment processes. For example, when setting a threshold for transaction monitoring, it is useful to analyze suspicious transaction reporting status and review the risk assessment for a given customer's nature of business or transaction pattern. FIs, then, shall increase the detection sensitivity by lowering the threshold for certain client types or transaction patterns taking into account their risks which are assessed as high.

The purpose of suspicious transaction report analysis is to improve the accuracy of risk assessment for FIs. Even if the number of notifications is small, if there is a possibility

that the reasons for the reporting seem to require other transactions to be reported as STRs (including, but not limited to, transactions with the same customer or similar transactions), review of the suspicious transactions review procedures may need to be conducted. Moreover, a lookback exercise needs to be conducted to confirm that transactions that should have been reported have indeed been reported and the results of the review documented in the risk assessment for increased AML/CFT control.

In addition, in cases where FIs identify a certain number of transactions which are applicable to "Reference Cases of Suspicious Transactions" but are not reported as suspicious transactions as a result of the sample checking, there is a possibility that the transactions that should be reported have not been detected or have not been reported. In such cases, audit, i.e. the third line should evaluate the control framework for filing suspicious transaction reports.

II-2 (2) Risk assessment

【Required actions for a financial institution: v】

Conduct the review of the risk assessment regularly, at least once a year, as well as when an event such as the emergence of new risks or the introduction of new regulation that may have a significant impact on AML/CFT measures occurs.

【Q】

Is it correct to assume that "regularly" means about once a year?

【A】

"Risk Assessment" should be reviewed at least once a year. In addition, when risks such as products/services, transaction types, country/region, and customer attributes change as new risks arise or new regulations are introduced, they need to be reviewed whenever necessary.

In addition, the timing and duration of periodic reviews are to be reviewed in advance and documented for increased effectiveness. When ad-hoc reviews are conducted, the situation in which such reviews are triggered is reviewed in advance and documented, which should ensure greater effectiveness.

In addition, customer risk assessments shall be conducted at a frequency based on the risks related to, and in case an event that materially affect the client's risks, an immediate risk assessment shall be conducted. Therefore, methods for detecting such events affecting customer risk assessment, criteria, and procedure, etc. shall be documented in advance with notification to the first line and other departments.

II-2 (2) Risk assessment

【Required actions for a financial institution: vi】

Involve the Board in the processes of risk assessment, and obtain approval from the Board for documenting the results of the risk assessment.

【Q】

It states "involve the Board in the processes of risk assessment" and please advise on which aspects and to what extent in which the Board must be involved with examples.

【A】

During the ML/FT risk assessment stage, the Board is required to: (1) ensure a framework for evaluating ML/FT risk through firm-wide cooperation and collaboration, (2) coordinate the interests of each department at the Board level, (3) provide guidance and support for conducting smooth and effective ML/FT risk assessment, and (4) take the initiative in making decisions on the allocation of resources that enable the above.

As an example, the board member responsible for AML/CFT shall approve the review and execution of the assessment methodologies, confirm that the risk assessment process is properly structured and implemented, and, if necessary, improve these assessment methodologies and their implementation without delay... The Board, during the risk assessment process, needs to receive updates from the responsible department(s) from time to time and discuss and approve the risk assessment result and finalize the assessment.

II-2 Identification, assessment, and mitigation of risk

(3) Risk mitigation

(i) Objectives and Implications of Risk Mitigation Measures

【Required actions for a financial institution: i】

Collect and verify information about customers and their activities and transactions (Q1), compare that information with the results of risk assessment (Q2), and determine and implement effective measures to mitigate those identified risks (Q3, Q4, Q5).

【Q1】

When investigating information about "customers and their activities and transactions", please advise what should be kept in mind.

【A】

There are various measures available for investigating "customers and their activities and transactions". For example, one can analyze the products and services used by the individual customer; the transaction records; and asking the individual customer to provide attestation or obtain evidence on a risk-basis. Further, obtaining negative media information and performing subsequence investigations is possible without client contact when such information affects the customer's risk. Such investigation into the background and status may be required, along with reviewing the customer's transactions against historical transactions, occupation, or purpose of transactions for their consistency.

In any case, methods for investigating "customers and their activities and transactions" shall be decided depending on the nature of their customer and transactions, on a case by case basis.

【Q2】

Please advise on the points to note when comparing information about "customers and their activities and transactions" and the "the results of risk assessment"?

【A】

First, based on available information about the customer and transactions, set a preliminary risk rating and then update that assessment with the latest information of the customer attributes and customer transactions. Conducting an appropriate customer risk assessment would enable a financial institutions to determine and apply sufficient risk mitigation measures.

【Q3】

Please advise on the points to note to “determine and implement effective measures to mitigate those identified risks” and please provide possible measures.

【A】

When determining which risk mitigation measures to be implemented, it is important to comprehensively assess and apply measures based on effect of mitigation measures solely focusing on ML/FT risks and additional effect derived from various other measures already embedded for other purposes.

For instance, verification at the time of transaction for deposit account opening is effective in preventing transactions with a party suspected of pretending to be a customer through identity verification. In conjunction with such measures, conducting customer risk assessment and deciding beforehand on the items to obtain further information, on a risk-basis, and documenting the procedures for enhanced due diligence together with facilitating its understanding and implementation can be regarded as risk mitigation measures for onboarding. Even after onboarding, reviewing customer risk on a risk-basis frequency and when certain events occur that increased the customer’s risk, along with conducting transaction monitoring by applying/adjusting risk-based threshold can be regarded as risk mitigation measures. In addition, upon a thorough review of customer information, for instance, if the customer is requesting to open an account at a branch far from place of residence or work, without justifiable reasons, then additional information must be thought and upon comprehensive assessment, either to reject or put on hold the request, under freedom of contract principle, is thought to be a risk mitigation measure.

In addition, in particular, in cases where there are many cases of early unauthorized use after accepting customers such as opening accounts, and similar situations are clearly seen, one possible risk mitigation measure could be to limit the type and amount of transactions allowed for a certain period after opening, for example.

When considering risk mitigation measures it is important to implement required measures commensurate with the business activities.

【Q4】

For internet banking, please advise on the points to note regarding ML/FT risk assessment and mitigation measures.

【A】

Internet banking requires measures taking into account non-face-to-face transaction risks, such as account being compromised, transaction with a party suspected of pretending to be a customer, or possibility of being presented false information at the time

of account opening. Therefore, implementing countermeasures to prevent suspicious access would be duly considered, such as monitoring if following information tally with its customer attribute: device information including IP address; browser language; time zone; combination of User Agent information (such as combination of OS/browser); and screen resolution information.

【Q5】

Please advise on the points to note regarding ML/FT risk assessment and mitigation measures for payment for imports and exports, wire transfers, and payroll payment.

【A】

Future-dated payments such as ones for imports or exports, wire transfers request for future value, and payrolls are conducted automatically on the transaction date upon request of such future-dated payments. In case where funds for future-dated imports or exports, wire transfers, or payroll payments are not received or balance is short of the required amount, decision must be made not only from a credit perspective but also taking into account ML/FT risks from transaction details obtained during the transaction application process.

For example it is necessary to confirm that the client's transaction representative is not pretending to be a customer or the account has been compromised.

Moreover, risk-based measures must be taken in cases where customers' requests lack valid justification, where multiple future-dated wire transfers or payroll requests are made, different from previous counterparties, or cross border payments are requested without links to its business activities.

II-2 (3) (i) Risk mitigation measures

【Required actions for a financial institution: ii】
Undertake enhanced mitigation measures in cases where ML/FT risks are high, commensurate with the level of risks posed by individual customers and their transactions, in accordance with policies, procedures, and execution plans developed by the financial institution.

【Q】

What are the specific measures required to" Undertake enhanced mitigation measures in cases where ML/FT risks are high, commensurate with the level of risks posed by individual customers and their transactions, in accordance with policies, procedures, and execution plans developed by the financial institution."?

【A】

Based on the pre-defined institutions' ML/FT related policy, procedure, and execution plan that outline risk-based mitigation measures for high risk customers, specific timing in which such measures are implemented, person in charge, processes, and department in charge, applying risk-based mitigation measures is required. This risk-based mitigation measures include risk assessment of individual customers and conducting risk-based transaction monitoring.

For instance, in case ML/FT risk is perceived to be high, in addition to making decision based on the standard due diligence process, documenting beforehand the enhanced risk-based mitigation measures, such as asking for evidence of the purpose of transaction or the source of funds can be considered.

II-2 (3) (i) Risk mitigation measures

【Required actions for a financial institution: iii】
Examine updated cases and information from domestic and foreign authorities and industry associations, as well as the items listed in the Guidelines, and then undertake mitigation measures commensurate with the risks the financial institution faces.

【Q】

What are the specific measures requested under "Examine updated cases and information from domestic and foreign authorities and industry associations, as well as the items listed in the Guidelines, and then undertake mitigation measures commensurate with the risks the financial institution faces."?

【A】

Collecting broader range of information allows for more effective risk mitigation. Therefore, financial institutions need to review not only the NRA and the AML/CFT Guidelines, but also publications related to ML/FT risks published by industry associations and domestic and foreign authorities for possible mitigation measures that is commensurate with the risks the financial institutions face, and apply appropriately.

II-2 (3) Risk mitigation

(ii) Customer due diligence (CDD)

【Required actions for a financial institution: i】

Formulate a **customer acceptance policy (Q1, Q2, Q3)**, based on the risk identification and assessment of the institution, to systematically and specifically identify and determine high-risk customers and transactions and required actions for them.

【Q1】

This asks for formulating a "customer acceptance policy" but please confirm that it does not ask to document a procedure titled "customer acceptance policy," but rather asking to document it within a procedure about a risk based customer acceptance policy?

【A】

With regards to the AML/CFT Guidelines II-2(3)(ii)【Required actions for a financial institution :i】, it does not automatically ask for creating a document titled "customer acceptance policy," but the intention is to ask the financial institution to explicitly define the customer acceptance policy and its procedures and document them along with facilitating their thorough understanding especially to the first line.

The document structure of the policy shall be decided per each financial institution.

【Q2】

What needs to be included in the "customer acceptance policy"?

【A】

Based on its own risk identification and assessment, clients or transactions deemed to be of higher risk and corresponding actions to the customer needs to be explicitly included to facilitate decision making. In addition, in case rejection or restriction on transaction will be implemented, appropriate approval authority shall be included.

【Q3】

What are the points to take note for "acceptance" of walk-in customers?

【A】

For walk-in customers (1) taking appropriate action defined in relevant laws, (2) appropriately taking risk-based actions, (3) conducting thorough client explanation, are considered to be important.

For (1) it is required to ensure obligations stipulated in APTCP are fulfilled.

For (2) it is required to ensure that pre-defined risk mitigation measures are

implemented to the walk-in customer, derived based on comprehensive and specific risk assessment of products/services, transaction types, countries/geographic areas, or customer attributes and applying it to the walk-in customer.

Both (1) and (2) requires appropriate actions upon conducting verification at the time of transaction for customer information, as per the legal requirement, such as name, date of birth, address, and once the customer is identified as an anti-social force or a sanctioned party, the financial institution is required to follow freedom of contract principle, internal procedures, and legal requirement to reject the request and take appropriate measures such as submitting a suspicious transaction report. In addition, upon transaction screening, if there is suspicion of a match as an anti-social force or a sanctioned party, discussion with senior management is required to decide on approval/rejection of the transaction and submit a suspicious transaction report. It is also required to create a framework that allows the financial institution to identify when the same walk-in customer conducts transaction at a different location.

Additionally, for instance, if a walk-in customer who requests for a transaction at branch A is rejected due to being an anti-social force or a sanctioned party, a framework must be established to appropriately prevent a transaction by the same walk-in customer attempting to transact in branch B or elsewhere.

For (3), a walk-in customer does not have previous transaction and thus information is limited, possibly resulting in the processes for (1) and (2) to be time consuming. Thus it is important for the financial institution to thoroughly explain to the customer the procedure and the time it will take and have the client understand.

In case where a through explanation is provided to the client but there is no cooperation, a high-value transaction, different from the stated purpose of transaction, is requested without a reasonable background, or a transaction is deviating from customer attributes, it is necessary to follow an internal policy to ask for senior management decision on the matter.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: ii】

When formulating the customer acceptance policies in i. above, consider customers' and **beneficial owners' (Q1)** occupations and business activities and **other various information (Q2)** such as their backgrounds, assets and incomes, sources of funds, countries/regions of residence, products and services of their use, and their forms of transactions.

【Q1】

Can we regard the definition of beneficial owners same as the one defined in APTCP?

【A】

Such understanding is correct but for the verification method, depending on the result of client risk assessment, in addition to client attestation of the beneficial owner, it is not intended to prevent additional measures such as obtaining evidence of the beneficial owner, which exceeds the requirement set out in the law.

【Q2】

Are information such as beneficial owner's occupation and business activities indicated in the AML/CFT Guidelines examples of information to be analyzed and based on it financial institutions must formulate its own customer acceptance policy taking into account the size and nature of their business?

【A】

All items listed in the AML/CFT Guidelines II-2(3)(ii)【Required actions for a financial institution: ii】are examples and the intention is not to uniformly ask for verification or consideration of all items for all customers or beneficial owners.

In any case, a risk-based process based on customer risk assessment is required, such as obtaining evidence for higher risk customers for deep-dive investigation, when determining how and what information to verify and consider, rather than uniformly applying the minimum standard set out in the law or the Guideline.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: iii】

Seek reliable evidence (Q3) when surveying information relevant to a customer and its **beneficial owner (Q1)** and the purpose of transaction, including **identity information (Q2)** of the customer and beneficial owner and other information such as the occupation and business details, personal history, the state of assets and incomes, source of funds, country/region of residence, etc.

【Q1】

Please advise on the points to note when surveying about beneficial owner's identity information.

【A】

As described in II-2(3)(ii) Customer Due Diligence (CDD) main paragraph, when financial institutions conduct a transaction with a customer, basic information such as who the beneficial owners are and deciding and implementing appropriate risk mitigation measures are critical.

Therefore, not only at start of the relationship, a risk-based approach on verifying the identity information of the customer's beneficial owner is required during ongoing CDD.

【Q2】

Is obtaining "reliable evidence" for identity information verification the same as "identity verification items" in APTCP?

【A】

The term "identity information" in the AML/CFT Guidelines encompasses a broader range of items such as, the client and its beneficial owner's occupation and business details, personal history, the state of assets and incomes, source of funds, country/region of residence, which is broader in scope than "identify verification item" defined in APTCP. The intention is not to uniformly require each items for all clients or beneficial owners, but a risk-based approach on which items to verify and consider needs to be discussed and documented beforehand to ensure effectiveness.

【Q3】

What are examples of “reliable evidence”? For example, identification documents set out in Article 7 of the Ordinance for Enforcement of APTCP applicable for survey of identity information?

【A】

“Reliable evidence” refers to official documents or its equivalent that validates the authenticity of the customer declaration.

When conducting the survey of identity information, identification documents set out in Article 7 of the Ordinance for Enforcement of APTCP and documents verifying the personal history and the state of assets and incomes can be leveraged along with other documents depending on the items to verify. For example, a shareholder registry, annual securities report, and appendix for corporate tax return may be requested, or the notary public's Articles of Incorporation authentication scheme (Note 1) to declare beneficial ownership and the Beneficial Owners List System (Note 2) may be used. An example would be at time of payout of a life insurance, if the beneficiary is an organization, a survey of the beneficial owner can be conducted by obtaining evidences such as shareholder registry or annual securities report. However, in cases where financial institutions seek reliable evidences, it is necessary to obtain and validate multiple documents as needed.

In addition, for survey on the purpose of transaction, if the purpose is for commercial use, obtaining transaction record with the counterparty or contracts for the transaction may be considered.

For items defined in APTCP, verification must be conducted in accordance with the method and documents stipulated in the law and risk-based decision on obtaining additional evidence needs to be made.

It is also important to establish a mechanism to confirm the authenticity of "reliable evidence" since there have been confirmed cases in which deposit accounts, accounts, etc. are fraudulently created through the falsification of identity verification documents (driver's license, etc.) and the accounts are used for ML/FT.

(Note 1) At time of incorporation, certification of the Articles of Incorporation requires declaration of its beneficial owners (started on 30 November, 2018 due to the enforcement of the revised Regulation for Enforcement of the Notary Act).

(Note 2) Commercial registry offices retain the document containing the beneficial ownership information of stock companies upon request from them, and issue a copy of the document (started on 31 January, 2022 due to the enforcement

of Rules on the Retention of the List of Information on Beneficial Owners at Commercial Registry Offices).

【Q4】

When surveying identity information and the purpose of transaction of a customer and its beneficial owner, “reliable evidence” is being requested, but is it mandating to uniformly collect evidence, not only using client declaration, even in cases where the law does not?

【A】

When surveying information on a customer and its beneficial owner’s identity information and purpose of transaction, the intention for asking “reliable evidence” is to ask for evidence taking into account the validity of declaration made by the client. Therefore, a risk-based approach must be taken to obtain evidence to confirm the validity of the client’s declaration and not to uniformly ask for documents on wide-ranging items.

However, such measures must not be conducted sporadically and criteria and procedure for taking such measures must be documented beforehand to ensure effectiveness.

For items defined in APTCP, verification must be conducted in accordance with the method and documents stipulated in the law and risk-based decision on obtaining additional evidence needs to be made.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: iv】

Comply with laws and regulations related to Japanese and other foreign sanctions, such as by screening the names of customers and their beneficial owners with sanctions lists compiled by the relevant authorities, and **take other necessary measures according to the risks involved**.

【Q1】

Please advise on the points to be noted to "Comply with laws and regulations related to Japanese and other foreign sanctions" and "take other necessary measures according to the risks involved."?

【A】

With regards to compliance with domestic and international laws and regulations, for example, FIs are required to confirm that there are no transactions with the designated names exist, or are required to freeze such assets in case there is a transaction with entities or persons designated by United Nations Security Council (hereinafter referred to as the "UN Security Council") resolutions, pursuant to Articles 16 and 21 of the Foreign Exchange Act, once the Ministry of Foreign Affairs has issued an Official Gazette based on the resolution. Moreover, taking into account international standards (see Note), even before the Ministry of Foreign Affairs' issuing the Official Gazette, when sanctioned persons or entities pursuant to a UN Security Council resolution is added or its information updated, FIs are required to update their list without delay and conduct screening against its customers; in case a potential match with the sanctions list exists, appropriate and cautious measures including enhanced due diligence is to be conducted to confirm whether the hit is a true positive match or a false match with merely identical names.

Furthermore, a specific country or region could impose economic sanctions against a specific country or region without a resolution of the UN Security Council. FIs should note that careful investigation could be required to ensure that the persons, goods, and services involved in the transactions are not related to sanctions imposed by a specific country or region.

Therefore, it is important for a FI to maintain database or system and obtain human/financial resources, commensurate with the risk that the FI faces, to ensure that the above measures are duly conducted.

Recently there have been reports of ransomware infections, which require ransom for

data recovery. Internationally it has been pointed out that ransomware ransom can be misused for terrorist financing. In the US, a recommendation was issued to FIs to alert them to the risk of sanctions for involvement in the payment of ransomware ransom. There are no borders in the cyber world and ransom payments shall not be processed by FI; FIs must understand that such terrorist financing risks are present for customer wire transfers.

(Note) FATF requires funds and assets held by persons or entities designated under UN Security Council resolutions to be frozen, without delay, as part of economic sanctions against terrorist financing or proliferation of weapons of mass destruction.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: v】

Establish a framework to properly detect **high-risk customers (Q2)** in accordance with the size and characteristics of the financial institution, by **utilizing reliable databases and systems or other reasonable measures (Q1).**

【Q1】

It states "utilizing reliable databases and systems or other reasonable measures" and can we understand it implies implementing PEPs database and AML system generally provided by vendors?

【A】

It can be understood that database, including those provided by external vendors which provides reliable source of PEPs, persons, countries, and entities designated under UN Security Council resolutions, sanctions list of countries and regions relating to transactions, database including Japanese anti-social forces, and AML systems in general are examples. In such case, list update must be conducted without delay, transaction filtering system's list and fuzzy logic and transaction monitoring system's scenario and threshold must be adjusted appropriately, commensurate with risk.

【Q2】

It states "Establish a framework to properly detect high-risk customers" and are foreign PEPs included in the definition of "high-risk customers"?

【A】

In general, foreign PEPs have the risk of potentially conducting corruption and they shall be included in the high-risk customer type and maintained. Therefore, financial institutions are required to appropriately maintain a framework to identify foreign PEPs but the detailed scope of high-risk customers and identification method shall be considered by individual institutions, commensurate with the business nature and appropriate action shall be taken accordingly.

For foreign PEPs, risk assessment needs to be conducted taking into account the position and the role. In case the PEP is no longer in active service, taking into account the period out of the service (regardless of the length) will allow for a more detailed ongoing CDD.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: vi】

Conduct customer risk assessment for all the customers (Q1-7) based on the results of the assessment of the risk of ML/FT for products/services, transaction types, countries/geographic areas, customer attributes, etc. (risk assessment to be conducted in II-2 (2)), and determine the mitigation measures to be taken **in accordance with the customer risk assessment (Q8, 9).**

【Q1】

It states "Conduct customer risk assessment for all the customers" but is it required to conduct customer risk assessment at time of initiating a transaction?

【A】

At time of initiating a transaction, not only approving or rejecting a transaction or determining head office escalation, conducting customer risk assessment for the purpose of ongoing CDD is required.

【Q2】

What are the methods to "Conduct customer risk assessment for all the customers"?

【A】

Customer risk assessment is regarded as a measure for all clients, based on the risk assessment taking into account ML/FT risks arising from products/services, transaction types, countries/geographic areas, and customer attributes.

The AML/CFT Guidelines requires financial institutions to conduct customer risk assessment on all their customers but the measures can vary based on the size and nature of the financial institution and its business profile. For example, conducting risk assessment based on "client group" who uses the same products and services or have similar customer attributes can be considered as well as conducting such assessments on "individual client" basis.

【Q3】

It is stated to "Conduct customer risk assessment for all the customers" but for long-term inactive account, irrespective of other factors, can they be treated as low risk without further review of customer attributes and apply different CDD measures from the standard one until the account becomes active, in which it will be treated as high risk, requiring

EDD, accompanied with update of client information?

【A】

The AML/CFT Guidelines requires financial institutions to comprehensively take into account the identified and assessed ML/FT risks and conduct customer risk assessment on all its clients, but for specific measures, financial institutions must evaluate on an individual basis taking into account the transaction and customer profiles.

For instance, for a client having a long-term inactive account, if the risk assessment has been conducted on the basis of having no transactions for an extended period, if the account activity remains the same, it can be assessed as low risk but if a transaction is suddenly initiated, a system needs to promptly identify it and the financial institution will need to review the background of the activity. The basis of this lies in the fact that the financial institution needs a framework to identify, regardless of value, transactions that are initiated by a long-term inactive account.

In addition, if such inactive account has become active, there could be illicit transfer or loan of the account and the financial institution must take into account such aspects and conduct a customer risk assessment and maintain a framework to determine whether EDD shall be immediately conducted.

【Q4】

For a small cooperative financial institution, comprised of members within the same region, occupation, or entity for the purpose of mutual assistance, in some ways the customer base is limited and transaction is conducted closely via face-to-face with client information obtained to a large extent. Is it acceptable, as part of the CDD process, to group all customers by groups such as members/non-members, corporates/individuals, living expense accounts/other accounts, and conduct risk assessment per each identified group and apply mitigation measures accordingly?

【A】

Taking into account the risk assessment based on the size and nature of business of the financial institution, if determined that risk is limited, it can be possible to conduct customer risk assessment per groups such as members/non-members, corporates/individuals, living expense accounts/other accounts. For instance, if the nature of business of the financial institution is of low risk and the customer base is limited by membership with customer representative understanding well the nature of each client, a customer risk assessment based on “customer group” can be perceived as sufficient.

【Q5】

Can a phased approach taken in which we initially classify “perceived to be relatively higher risk clients” and “perceived to be lower risk clients” and over a period of several years, collect, accumulate, and analyze client information and conduct a more detailed risk assessment such as low, medium, and high risk for the purpose of enhancing ongoing CDD?

【A】

For customer risk assessment, a financial institution can first conduct risk assessment based on the information at hand, and based on the result, an ongoing CDD shall be conducted, updating customer information as the process moves forward. It may be appropriate that during this process, the initial risk assessment of breaking down into high risk and low risk client groups can then evolve to a more sophisticated approach. For a specific measure, it must be decided upon taking into account individual factors of the financial institution, including size and nature of business. If customer information collection, accumulation, and analysis processes are to be conducted over a period of several years, a plan shall be set and progress shall be tracked.

【Q6】

When conducting customer risk assessments through customer grouping, what are the possible groups? In addition, please advise on a client group considered to be higher risk.

【A】

The customer grouping analysis conducted by individual financial institutions as part of the customer risk assessment process will vary depending on risk from entire business operations, but for instance, customer attributes such as anti-social forces and sanctioned persons shall be treated as “do not trade” customers and for customers with records of STR filing, suspicion on illicit account usage, or with negative media shall be treated as high risk.

Apart from this, for instance, details of transaction and situation can be used for grouping, in which customers using products/services assessed as high risk to be treated as high risk clients. In addition, inactive accounts, until they become active, can be treated as low risk whereas existing accounts for which the identity of the customer has not been verified based on some official documents or some other reliable identification documents, individual’s account used by a corporate, or accounts used for illicit purposes, shall be treated as high risk and per a procedure that has been documented beforehand, a review of customer information shall be conducted.

For central and local government organizations it is possible to uniformly treat them

as low risk. For organizations that are managed by central or local government organizations, upon review of the history of foundation, details of transaction, relationship with the central or local government organization, and nature of business, it is possible to treat them as low risk as well.

【Q7】

Please advise on the points to note when assessing the risk of a customer who falls into the category of an organization.

【A】

When assessing the risk of a customer who falls into the category of an organization, it would be desirable to take into account the ML/FT risk of not only the organization but also the group as a whole, including the group formed by the organization, in light of the actual status of customers and related circumstances.

The guidelines require the customer risk assessment to take into account the customer attributes. Therefore, the organization to which the customer belongs (e.g., anti-social forces and their front companies) should be included in the factors to be considered when determining the customer attributes. Similarly, for a customer who is an organization, it is useful that the customer risk assessment is conducted taking into account the characteristics of the group to which the organization belongs or is formed by the organization. The definitions of "organization" and "group formed by the organization" should not be automatically determined but should be individually and specifically determined taking into account factors such as the characteristics of the organization and the group themselves, as well as the organization's position within the group or power on the group .

The definition of "organization" is not limited to legal entities, and unincorporated associations are also included. As other examples, an association that does not fall into the category of unincorporated associations because it does not have any unified decision-making body may be considered as an "organization." In addition, the definition of "group formed by the organization" should not be determined automatically based on the equity interest, including whether it is a (consolidated) subsidiary or an equity method affiliate, but should be determined based on the risk without taking into account the arrangements such as capital relationships, contracts and agreements. For example, when a person (anyone other than the customers) who does not have any capital relationship with the customer established a joint venture with the customer and the risk level of the person is defined as high, these circumstances may be considered when determining the risk level of the customer. In addition, when the beneficial owner of the customer is also the

beneficial owner of a high risk customer, it may be considered that the customer and the high risk customer form a group.

When conducting customer risk assessment for an organization, it may be appropriate to consider not only the ML/FT risks of the organization but also those of the entire group of the organization taking into account other organizations whose beneficial owner is the same natural person as or the spouse of the beneficial owner of the organization, or that have a capital relationship or relationship based on certain legal arrangements. Specifically, if there are entities whose risk might have an impact on the risk level of the organization (e.g. entities conducting transactions in areas neighboring sanctioned regions), the risk level of the organization should be assessed taking into account the risk of the entities.

In any event, it is important to conduct customer risk assessment by identifying the actual status of the customer and taking into account the circumstances of the customer carefully.

【Q8】

Please advise on the points to note in case the financial institution is accepting foreign residents.

【A】

For customers who are foreign residents with a period of stay, on a risk-basis, CDD must be conducted in accordance with the customer risk.

In addition, in case termination of account is expected in the future, including the case for foreign residents, an identification of risk and assessment for the account being sold and used in crime and appropriate risk mitigation measures must be applied.

As for foreign residents with a period of stay, as a risk mitigation measure, it is necessary to check the period of stay and maintain it in a CDD system. Also, it is necessary to request the customer to close the account before the expiration of the period of stay in case the customer does not renew the period of stay, furthermore, to notify the renewed period of stay in case the customer extends it.

When an extension of the period of stay is verified, a possible measure by a financial institution could be updating the CDD information in the system. On the other hand, if any heightened risk is identified, such as the extension not being verified, a possible measure could be taking risk mitigation one, for instance some transaction restrictions.

In any case, it is necessary to determine how to manage customers with a fixed period of stay based on the risks they face, and it would not be appropriate to decide not to implement the above request before the expiration of the period of stay, without any

appropriate review process based on the risks related to.

For Special Permanent Residents and Permanent Residents, there is no risk based on the period of stay, yet similar to other customers, client risk assessments are required.

In case a foreign resident with a resident card applies for permission to extend the period of stay or permission to change status of residence (hereinafter referred to as "application for extension of period of stay, etc.") and the disposition pertaining to such application is not made by the expiration date of the period of stay, the foreign resident may continue to stay in Japan with the previous status of residence until the time of the disposition or the expiration date of two months from the expiration date, whichever comes earlier. When an "application for extension of the period of stay, etc." is filed, the fact that the application is pending will be indicated on the back of the resident card in the "Application for permission for extension of period of stay, etc. column" (except in the case of online application). When considering risk-based measures, it is necessary to be aware of the existence of such a rule.

【Q9】

How should CDD for domestic PEPs or persons who are or have been entrusted with a prominent function by an international organization be performed?

【A】

Financial institutions, etc. are required to conduct customer risk assessments for all customers and conduct CDD in accordance with the risks.

This also applies to domestic PEPs and persons who are or have been entrusted with a prominent function by an international organization (Note). For domestic PEPs or persons who are or have been entrusted with a prominent function by an international organization, using information obtained during account opening or ongoing CDD, similar to other clients, customer risk assessments shall be conducted and risk-based measures stipulated in II-2 (3) (ii) of Guidelines for AML/CFT shall be taken.

(Note) Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions. International organizations are entities established by formal political agreements between their member states that have the status of international treaties.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: vii】

For customers determined to be of high ML/FT risk (Q1), apply enhanced due diligence (EDD) measures in accordance with the customer risk (Q2) including the following:

a) Obtain additional information in accordance with the risk, especially that of customer's state of assets and incomes, purpose of transactions, occupation, title, and source of funds

b) Obtain the approval of **senior management (Q3)** for transactions with such customers;

c) **Enhance transaction monitoring by tightening the threshold for transactions conducted by such customers and increase the frequency of periodic reviews of CDD information (Q4)**, in accordance with the risk; and

d) Examine the need to assign stricter customer risk ratings for other customers with similar attributes. (Q5)

【Q1】

Does the term "customers determined to be of high ML/FT risk" refer to a customer who conducts high risk transactions defined in the first part of Paragraph 2 of Article 4 of APTCP which requires enhanced due diligence (herein after referred to as "high risk transactions"? Or does it add on to that definition or introduce new definition for high risk clients who do not conduct high risk transactions?

【A】

"Customers determined to be of high ML/FT risk" in the AML/CFT Guidelines II-2(3)(ii)【Required actions for a financial institution: vii】are customers regarded by the financial institution as high risk at time of onboarding, upon review and survey of the necessary information per its customer acceptance policy, as well as those identified as high risk during the course of ongoing CDD in which risk reassessment was conducted according to a pre-defined procedure.

It shall be noted that when conducting high risk transactions defined under APTCP, to meet legal obligations, confirming each points required under the law is a minimum requirement.

【Q2】

Are there instances, depending on the risk assessment, in which a higher level of due diligence is required for specified transactions (Article 7 of Order for Enforcement of APTCP. Also including transactions requiring special attention defined in Article 5 of the Ordinance for Enforcement of APTCP), than what is specified as part of the requirement for verification at the time of transaction? Also is a higher degree of enhanced due diligence for transactions requiring special attention defined in Article 12 of the Ordinance for Enforcement of APTCP being required for verification at the time of transaction?

【A】

Under the risk-based approach CDD framework, conducting transaction due diligence per APTCP is a minimum requirement and applying additional measures will certainly be required. Each financial institution, taking into account its size and characteristic, shall take appropriate measures per the objective of this Guideline.

【Q3】

What positions are intended for when referring to "senior management"? Is this synonymous with AML/CFT Officer defined under Article 11-3 of APTCP?

【A】

In the AML/CFT Guidelines, "senior management" includes for instance head of the department in charge of AML/CFT but each financial institution needs to make decision individually, taking into account its size and organizational structure. Please note that the definition is not necessarily synonymous with AML/CFT Officer defined under Article 11-3 of APTCP.

【Q4】

What specific measures are requested under "Enhance transaction monitoring by tightening the threshold for transactions conducted by such customers and increase the frequency of periodic reviews of CDD information"?

【A】

Taking into account the customer risk assessment conducted to all customers, for high risk customers, applying tighter thresholds for transaction monitoring or applying high-risk-customer-specific scenario can be considered on a case by case basis. For low risk customers, on the other hand, a lenient threshold or scenario can be considered.

Additionally, changing the contents, type, and depth of information to be collected

during ongoing CDD can be conducted as well.

【Q5】

What specific measures are requested under "examine the need to assign stricter customer risk ratings for other customers with similar attributes."?

【A】

Upon a customer risk assessment, for customers identified as high risk, products/services, transaction type, country/region, and customer attributes shall be reviewed and checking other customers for similar or identical attributes shall be conducted and once identified, considering the necessity to reassess such customers' risk rating shall be required.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: viii】

Additional measures (Q2), such as understanding the actual business status and geographic areas, etc., should be taken prior to the start of transactions or when conducting large transactions, in cases where there is a high risk of transactions, etc., such as where **the customer's business, geographic area, etc., is deemed to be irrational in light of the purpose of transactions, transaction pattern, etc. (Q1)**

【Q1】

What are the specific examples of "the customer's business, geographic area, etc., is deemed to be irrational in light of the purpose of transactions, transaction pattern, etc."?

【A】

The cases transactions identified as high risk, including the cases in which the customer’s office is remote from the financial institutions etc. where the transaction is applied without a legitimate reason, in which a third party who is not the importer or the payer of the business transaction applies remittance without a legitimate reason, and in which details of transactions are not align with the information declared by the customer.

【Q2】

What are the specific examples of additional measures which should be conducted when "the customer's business, geographic area, etc., is deemed to be irrational in light of the purpose of transactions, transaction pattern, etc."?

【A】

For the transactions that "the customer's business, geographic area, etc., is deemed to be irrational in light of the purpose of transactions, transaction pattern, etc.", financial institutions, etc. may request rational explanations and evidences to the customer, and visit the customer or conduct fact-finding visit. At least, financial institutions, etc. should identify actual business and locations of the customer in such high risk cases.

If the customer refuses the request for additional measures, financial institutions, etc. should carry out processes such as obtaining approval of senior managers for transaction until the information deemed to be irrational is clarified. At any rate, financial institutions, etc. should determine the additional measures for high risk transactions into account the features and the risks of the transactions.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: ix】

For customers determined to have low ML/FT risk, give due consideration for smooth execution of transactions by implementing **simplified due diligence (SDD) measures (Q1-Q6)** taking into account the nature of the risk, such as varying the scope, methods, and frequency of investigation and updating of customer information, while taking into account the characteristics of such risk; Raising the threshold for monitoring transactions conducted by such customers may also be considered.

【Q1】

Please provide specific examples which are recognized as “simplified due diligence (SDD) measures taking into account the nature of the risk”.

【A】

“Simplified due diligence (SDD) measures taking into account the nature of the risk” prescribed in the Guidelines means CDD measures applied to customers who meet certain conditions in the customers identified as “low risk” from the customer risk assessment, which retain proactive actions including review of customer information such as sending DM and instead monitor their transactions to confirm their risks remain low level.

【Q2】

What is the difference between “simplified due diligence (SDD) measures taking into account the nature of the risk” in the Guidelines and “simplified due diligence” in the APTCP (Article7, paragraph 1, main paragraph of the Order for Enforcement of APTCP and Article4, paragraph 1, main paragraph of the Regulation for Enforcement of APTCP)?

【A】

SDD in the Guidelines is a different concept from that prescribed in APTCP framework. SDD measures in the Guidelines are applied as measures of ongoing CDD at the time of review of customer information to understand actual status of the customers and review the results of customer risk assessment. Therefore it is different from “simplified due diligence” measures in APTCP which are applied when conducting a verification at the time of transactions.

【Q3】

What considerations apply when deciding on the scope of "simplified risk-based customer due diligence (SDD)"?

【A】

In general, customers that are considered to be at low risk of identity theft or fraudulent use are assumed to be subject to "simplified risk-based customer due diligence (SDD).

Further, the FSA believes that the following points need to be taken into account, and as long as they are in line with (1) through (3), they may be subject to SDD.

(1)Financial institutions, etc. should conduct customer risk assessment for all customers by considering all the ML/FT risks of their products and services, transaction types, countries and geographies, and customer attributes, and then select customers to whom SDD measures are applied from among low risk customers.

(2) Financial institutions, etc. should establish a control environment to monitor transactions by customers to whom SDD measures are applied and detect irregular transactions with a transaction monitoring system whose effectiveness is evaluated periodically and on an ad hoc basis.

(3) Necessary KYC and CDD shall be taken for customers subject to SDD as well, including conducting regulatory required KYC/CDD, and when customer information is updated, the customer risk assessment shall be reviewed and necessary on-going customer due diligence measures shall be taken (this does not preclude categorizing a customer subject to SDD again when a review of customer risk assessment is conducted for the customer subject to SDD).

After satisfying (1) to (3) above, financial institutions, etc. should analyze all the ML/FT risks of their products and services, transaction types, countries and geographies, and customer attributes, and then select customers to whom SDD measures are applied.
In addition, the following (Note 1) to (Note 3) may also be taken into account in the risk analysis.

(Note 1) Legal persons and individuals with business nature generally have a considerable number of persons involved, such as business associates and parent-subsidiary companies, and there is a reasonable possibility that transactions conducted by legal persons and individuals with a business nature may include proceeds from crime and support money for terrorists.

(Note 2) Financial institutions, etc. may not be able to appropriately perform risk assessment for customers whose identity has not yet been confirmed (i.e., customers with whom transactions started before October 1, 1990) or detection of their suspicious transactions due to inaccurate customer information. Therefore, it is necessary to analyze risks based on the fact that the identity has not yet been verified and on the transaction history data of the customer.

(Note 3) Customers who have been referred, or requested to freeze their accounts, from external agencies such as investigating authorities in the past year or who have filed any STRs in the past year may have risks, such as being involved in crime.

【Q4】

In particular, for what types of customers could be considered as "risk-based simplified customer management (SDD)"?

【A】

For example, accounts that are used for similar transactions on a recurring basis and whose transactions are consistent with the customer information held (e.g., payroll transfer accounts, mortgage repayment accounts, utility bill transfer accounts, and other accounts not used for business), etc., could be subject to the SDD.

In any case, we assume that it is necessary to determine which customers are subject to SDD after analyzing all the ML/FT risks of their products and services, transaction types, countries and geographies, and customer attributes.

【Q5】

If we decide to implement "simplified risk-based customer due diligence (SDD)," what kind of controls are we supposed to implement?

【A】

The term "simplified risk-based customer due diligence (SDD)" as used in these Guidelines means that, among customers who are determined to be "low risk" as a result of the customer risk assessment and who meet certain conditions, the Bank will suspend proactive measures such as sending DMs, etc. and updating customer information, and ensure that the risk of terrorism financing is maintained at a low level through transaction monitoring, etc., unless the Bank determines that the customer is a "money launderer," in which case the Bank will not take any action. The customer management measures to ensure that the risk of terrorism financing is maintained at a low level.

Even for customers who are subject to SDD, it is necessary to take proactive measures to update customer information and review customer risk assessment, as necessary, when the FI has contact with a customer in any Specified transactions; when it obtains adverse information; or when a transaction is unnatural in light of the transaction history up to now, etc.

Particularly, if there is an opportunity to update customer information that should be renewed or recorded, such as when a customer subject to SDD who hadn't went through KYC with official documents or other evidence visits a branch, it is necessary to establish

a framework for updating necessary information by taking advantage of such opportunity.

For the customers whose identity (including beneficial owner's information), the purpose of transactions, and occupation and business details have not been confirmed in accordance with the Ordinance for Enforcement of APTCP in October 2016, such customer's identity information can be collected in the way set out in the Ordinance for Enforcement above at various opportunities.

【Q6】

How can financial institutions, etc. manage customers of listed companies and national and local governments?

【A】

In cases where reliable information based on legal grounds is published on a regular basis, such as in the case of a listed company (securities report, etc.), Financial institutions, etc. may conduct customer risk assessment based on such information and implement risk mitigation measures in accordance with such risk assessment.

In the case of national and local governments and their affiliated organizations, (that are established and invest funds on a legal basis, etc.), it is not necessary to update information on a regular basis, but it is necessary to take measures in accordance with the Pillar of Article 11 of APTCP.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: x】

In addition to the required actions in "(v) Suspicious transaction reporting (STRs)" listed below, implement ongoing CDD measures including the following:

a. **Develop and implement ongoing CDD policies that include the scope and frequency of the review on customers information (Q1) (Q2) (Q3) (Q4)** taking into account the results of the institution's risk assessment and transaction monitoring with respect to transaction types and customer attributes in particular;
b. **Continually review the appropriateness of the scope and methods of the due diligence conducted for each customer in light of the customer's actual transactions and businesses as well as the results of transaction monitoring (Q5)**;
c. **Appropriately manage the records of investigations, including the communication with the customer, and share these with the relevant executives and employees (Q6)**;
d. Revisit customer information promptly when certain events occur that are assumed to increase the risk of each customer. In addition to this, **the frequency of periodic customer data refresh (Q7) (Q8) (Q9) should be different depending on the risk of the customer (Q10) (Q11)**; and
e. **Review and, as appropriate, update the customer risk rating (Q12) and apply risk mitigation measures based on customers' risk attributes (Q13) (Q14)** obtained in the process of ongoing CDD. Further, **conduct transaction monitoring reflecting the customer risk rating result through ongoing CDD (Q15)**.

【Q1】

When performing ongoing CDD, how should we handle existing customers who have not been managed before?

【A】

Ongoing CDD measures should be applied based on customer risk assessment for all customers by comprehensively and specifically examining all the ML/FT risks of their products and services, transaction types, countries and geographies, and customer attributes. Regarding customer risk assessment of the existing customers, customer information which serve the assessment should be reviewed periodically and on an ad hoc basis. And frequency of periodic review of customer information should be

commensurate with the risk level of the customer. To determine the risk level of the customer, financial institutions, etc. should perform tentative customer risk assessment based on the existing information to update customer information and then determine the risk level of the customer by the official assessment based on the updated information.

【Q2】

When conducting ongoing customer due diligence, what specific information do you "investigate"? For example, is it correct to say that reconfirmation of the identity of the customer, the purpose of the transaction, the occupation, the nature of the business, etc. would fall under this category?

【A】

First, the purpose of the "survey" is to review the customer risk assessment based on the survey results in order to take effective risk mitigation measures. Therefore, it is not necessarily necessary to uniformly update all information held on individual customers, but it is necessary to investigate the information necessary for risk management with respect to the same customer. In addition to the examples suggested above, the information to be investigated could include, for example, the status of assets and income of the customer and its effective controlling person, sources of funds, etc., depending on the risk of the customer

In addition to the information referred to in Q2, assets and incomes of customers and their beneficial owners, and sources of funds may fall within the scope. Especially, it is required to establish a framework to consider whether to file STRs for the case that the amounts of deposits and withdrawals are higher than what are to be expected unnaturally based on the assets and incomes estimated from customer attributes declared by the customers.

Financial institutions, etc. should individually and specifically determine what information is reviewed taking into account the customer risk level or characteristics of the transactions. However, in any event, it is required to perform necessary review to collect information requisite to assess customer risk.

Also, in-depth explanations of the need of the review to the customers are required when updating customer information as a CDD measure.

【Q3】

What methods can be considered for "surveys" when implementing ongoing customer due diligence?

【A】

The purpose of the "survey" is to review the existing result of customer risk assessment based on the survey results in order to take effective risk mitigation measures.
For example, while the most common method is to send a letter by mail and obtain responses from customers, other methods, such as face-to-face at branches or using an application developed to collect those information, can be considered as appropriate to the risks involved.

In any case, it is necessary for FIs, etc. to consider and implement measures that can achieve the objectives of the survey according to the risks.

【Q4】

Could you tell us what you consider to be the "subject of the survey"?

【A】

Basically, all customers are subject to ongoing customer due diligence and are considered "subject to investigation.

However, long-term inactive accounts, such as accounts that have been inactive for more than one year, and existing customers who have been classified as non-transactional, require different control than other customers, but do not require periodic updates

【Q5】

What specific measures are required to "Continually review the appropriateness of the scope and methods of the due diligence conducted for each customer in light of the customer's transaction status as well as the results of transaction monitoring."?

【A】

It is required to establish a framework that internal audit division (the third line of defense) and control division (the second line of defense) continually check whether the scope and methods of the due diligence are appropriate in light of the customer's transaction status and the results of transaction monitoring, and consider whether to take actions such as reviewing the scope and methods of the due diligence and changing the risk level of the customer if necessary.

【Q6】

What specific measures are required to “Appropriately manage the records of investigations, including the communication with the customer, and share these with the relevant executives and employees.”?

【A】

To eliminate information disparity and implement efficient and effective AML/CFT measures, financial institution, etc. should not use the information obtained from the investigation only in the division responsible for AML/CFT but appropriately share it to all of their executives and employees according to the needs while complying with regulations.

【Q7】

Please provide specific examples of “customer information” which is required to review periodically.

【A】

The information to be reviewed by the periodic reviews and its frequency should be determined individually and specifically taking into account the risk level or the characteristics of transactions of the customer. For example, for high risk customers, the information on assets and incomes, sources of funds and business relation of the customer are reviewed in addition to the information to be reviewed for all customers annually and when certain events occur that are assumed to increase the risk of each customer. In addition, financial institutions, etc. should establish a framework in which the performance of the periodic review, including whether the information to be reviewed and frequency are effective, are examined and the system of the periodic review is modified if necessary.

【Q8】

Regarding methods of periodic review of customer information, is it appropriate to understand that the information not required any evidence to verify the declaration of the customers (e.g., when conducting normal identification and verification at the time of transaction for “beneficial owners”) by APTCP is allowed to be reviewed only based on the declaration of the customers?

【A】

The Guidelines require to obtain “reliable evidence” for the identification and verification of customers and their beneficial owners, and the intent of the requirement is to require obtaining necessary evidences to verify the declaration of the customers and

written evidences are not required without exception.

Anyway, when conducting the periodic review commensurate with the risk level of the customer, it is required to obtain evidences base on the risk level rather than uniformly by applying the minimum standards set by individual regulations and the guidelines.

【Q9】

Does “periodic review” of customer information require to make contact (by telephone, postal mail or others) with all the customers, including the customers identified as low risk and are applied SDD measures, to be interviewed or to provide documents with the objective of reviewing the identity and CDD information for AML/CFT purpose? Or, for such customers, is it allowed not to make contact to all of them but to determine the scope of the review based on the data on customer attributes and past transactions; and, if exist, discoveries from past operations?

【A】

Ongoing CDD should be performed to all the customers including customers identified as low risk. However, it is not necessary to perform at the same frequency and uniformly to all the customers, which means that the frequency, information to be obtained and methods of ongoing CDD should be individually and specifically determined depending on the risk level of the customer.

If information necessary for AML/CFT measures are identified on the occasions such as when the customers access the web site of financial institutions, etc. with the intention to have over-the-counter transactions, internet transactions, or update their information, or when financial institutions, etc. visit the customers periodically or on an ad hoc basis, it may be considered that the information of customers are reviewed for ongoing CDD.

However, please note that measures applied for ongoing CDD should be commensurate with the risk level of the customer, because the inspection of actual business status, onsite inspections or face-to-face communications are needed for certain high risk customers.

【Q10】

Please provide the specific frequency required by "the frequency of periodic customer data refresh should be different depending on the risk of the customer." In addition, is it appropriate to understand that this requirement does not require a comprehensive review of all customer information, but allow the performance of an in-depth review only when events that require the updating of the customer risk level are identified from certain information, such as the current address?

【A】

When performing ongoing CDD, it is not always required to review all information related to the customers, but it is required to individually and specifically determine the frequency, information to be reviewed, methods and other matters depending on the risk level of the customer.

Appropriate risk assessment based on the latest information is essential in order to determine and implement mitigation measures to be taken based on risk.

For example, customer information may be reviewed at the frequency of once a year for high risk customers, once every two years for moderate risk customers and once every three years for low risk customers. Not limited to this example, financial institutions, etc. may decide the frequency at their own discretion.

Information to be reviewed is determined with the objective of obtaining information necessary for customer risk assessment, taking into account the individual and specific situations. When reviewing information, public information may be referred to and confirmation with customers may be conducted.

When performing ongoing CDD, it is important that the first line and second line of defense cooperate and take appropriate control when managing the schedule of the review of customer risk assessment; managing the customers for whom the information review cannot be completed by the due date; and making up for the delay in schedule. Also, it is expected that the management status of delay in schedule is periodically reported to the management and measures to make up for the delay are taken.

【Q11】

What considerations could be made, if financial institutions, etc. decide the frequency at their own discretion, not limited to the examples in Q10 (once a year for high risk customers, once every two years for moderate risk customers and once every three years for low risk customers)?

【A】

If, not limited to the examples in Q10 (once a year for high risk customers, once every

two years for moderate risk customers and once every three years for low risk customers), financial institutions, etc. decide the frequency of periodic customer data refreshes at their own discretion, it is necessary to verify the validity of the frequency from the viewpoint of conducting customer risk assessment appropriately, based on the premise that financial institutions, etc. have assigned risk ratings for all customers, and then periodically verify that there is no problem with the validity of the frequency.

Specifically, the following measures may be taken:

(1) Set a reasonable frequency to maintain appropriate customer risk assessment by analyzing risk indicators, such as the degree of increase in customer risk scores due to previous periodic reviews of customer information.

(2) Review customer information and customer risk assessment as necessary when events that increase customer risk occur.

(3) Investigate customers detected through transaction monitoring and filtering, and then review customer information and customer risk assessment as necessary.

(4) Confirm the effectiveness of the above measures on a regular basis (for example, annually), and review appropriate measures based on the results.

【Q12】

Is it possible to classify customers who initially defined as “high risk” based on their customer attributes or transaction types as moderate or low risk after reviewing information?

【A】

The risk level of customers should be reviewed periodically and on an ad hoc basis, and it is allowed to raise or lower the level.

Therefore, it is possible to classify customers who initially defined as “high risk” as moderate risk based on later change of situations such as change in transactions or additional information.

However, it is required to know actual status of the customers for such re-assessment, therefore, enhancement of the quality of inspection of customers’ actual status is required.

【Q13】

What specific measures are required to “review and, as appropriate, update the customer risk rating and apply risk mitigation measures based on customers’ risk attributes”?

【A】

When performing risk mitigating measures commensurate with the risk level of the customer, it is required not only to vary the methods of due diligence such as EDD, CDD

and SDD, but also to tune the thresholds or scenarios of transaction monitoring, as well as to vary the information to be obtained and methods of information gathering at the time of transactions commensurate with the risk level.

【Q14】

Regarding "review and, as appropriate, update the customer risk rating and apply risk mitigation measures based on customers' risk attributes," how should we review and update the customer risk rating in cases where the responses for the survey are unable to be obtained from customers?

【A】

For the customers whose information must be periodically refreshed, it is necessary to review customer information by taking all possible measures that are considered effective in reviewing information, taking into account the characteristics of customers and transactions.

In cases where the responses for the survey are unable to be obtained from customers despite all possible measures that are considered effective in reviewing information, financial institutions, etc. may analyze their customer's risk based on such facts and past transaction data, etc., and appropriately reflect the results in customer risk assessment.

Financial institutions, etc. may need to: analyze the risks of these customer groups based on their understanding of the facts, such as customers not responding to the survey, postal mail not reaching the registered address, etc.; reflect the results of the analysis in customer risk assessment; periodically verify the validity of the control and assessment results of these customer groups; report the results to the management; and take appropriate risk mitigation measures.

In addition, financial institutions, etc. should consider and determine the appropriate methods to review and update the customer risk rating according to the risks involved, because the inspection of actual business status, onsite inspections or face-to-face communications are needed for certain high risk customers.

Also not limited to high risk customers, postal mail not reaching the registered address means a part of customer identity is unknown. The measures to address the situation where postal mail does not reach the registered address should be implemented on a priority basis, especially when financial institutions, etc. are unable to make contact with such customers, and when their accounts are active.

【Q15】

What specific measures are required to “conduct transaction monitoring reflecting the customer risk rating result through ongoing CDD "?

【A】

Regarding transaction monitoring, it is required to take measures such as tuning of thresholds or scenarios of the transaction monitoring to reflect the risk level of the customers.

II-2 (3) (ii) Customer due diligence (CDD)

【Required actions for a financial institution: xi】

For customers and transactions **with which CDD measures a financial institution determines to be adequate cannot be completed (Q2)**, including cases where the customer refuses to provide requested CDD information, consider appropriate **measures to eliminate the risk (Q1)**, such as rejecting the transaction. In such instances, financial institutions are required to assure that the customer or transaction are not refused or rejected **without a legitimate reason (Q3)** and that AML/CFT requirements are not used as an excuse for rejecting the customer.

【Q1】

Are the rejection of account opening for new customer, the closure of account and elimination of the transaction for the existing customer included in "measures to eliminate the risk"? Should we consider to reject transactions when account opening; money order; deposits and withdrawals; and money exchange are applied?

【A】

The measures and transactions mentioned in this question can be included because this article does not limit the customers and transactions to be considered whether to reject.

【Q2】

Is it appropriate to understand that the situation where we cannot prove that the funds are criminal proceeds but their actuals are unclear fall within a scope of "with which CDD measures a financial institution determines to be adequate cannot be completed" set forth in the "Required actions xi"?

【A】

The situation mentioned in this question may be a factor that raises ML/FT risk, however, it should be determined individually and specifically whether a situation fall within a scope of "with which CDD measures a financial institution determines to be adequate cannot be completed" taking into account the policy of financial institutions, etc. and the risk level the customers.

In addition, customers or transactions should not be refused or rejected only by the name of AML/CFT without a legitimate reason. Financial institutions, etc. should determine whether to refuse or reject them based on your rules for saving accounts or contracts with customers comprehensively.

【Q3】

Is it allowed that financial institutions, etc. determine whether they have a legitimate reason described in “customer or transaction are not refused or rejected without a legitimate reason” based on the risk taking into account the Guidelines and others?

【A】

Financial institutions, etc. should carefully consider the factors such as the situation and characteristics of each customer and the relationships with them when determining whether they have a legitimate reason based on their rules for saving accounts or contracts with customers in consideration of whether they can obtain information necessary for risk control.

In addition, they should obtain information on the situation and characteristics of each customer and the relationships with them as well as information necessary for risk control to the extent possible, and then, after employing every possible means, consider what restriction measures to be taken to the customer based on their risk comprehensively.

In implementing measures to eliminate the risk, it is necessary to conduct appropriate investigations, properly preserve the process and results of such investigations, and follow appropriate procedures at FIs.

It is also necessary to organize the contents of measures to eliminate the risk according to the circumstances, characteristics, and business relationships of each customer and information necessary for risk management that cannot be collected.

It is required to clarify policies and procedures regarding the content of that investigation, record keeping, procedures, and measures to eliminate the risk.

II-2 (3) Risk mitigation

(iii)Transaction monitoring and filtering

（Main paragraph）

In addition to CDD that focuses on individual customers, there is another approach for ensuring the effectiveness of risk mitigation measures, which focuses on the transactions to reduce risks through analysis of the actual transactions and the detection of unusual transactions and transactions subject to sanctions. It is essential for financial institutions to implement these approaches in combination to further increase the effectiveness of risk mitigation measures.

【Q】

Please provide the definitions of and differences between “monitoring” and “filtering”.

【A】

In the Guidelines, “transaction monitoring” refers to a method of reducing risk by detecting and investigating transactions deemed as unusual and confirming that they are unusual in light of past transaction patterns etc. and taking appropriate risk mitigation measures, or by filing STRs, as well as reflecting the results that a customer performed an unusual transaction in to the risk level of the customer. In addition, when a non-face-to-face transaction is conducted using communication means such as the Internet, it is necessary to conduct measures taking into account non-face-to-face transaction risks, such as the account being compromised, transactions with a party suspected of pretending to be a customer, and the possibility of being presented with false information at the time of account opening. Therefore, implementing countermeasures to prevent suspicious and unnatural access should be duly considered, such as monitoring whether the following information tallies with the customer attributes: device information, including the IP address; browser language; time zone; combination of user agent information (such as the OS/browser combination); and screen resolution information. The detection of such suspicious and unnatural access is also included in "transaction monitoring" in the Guidelines.

“Transaction filtering” is defined as a measure which, for example, mitigate the risk by screening the parties involved in the transaction and the existing customers against the lists of anti-social forces and sanctions, and then preventing the transaction by anti-social forces or sanctioned persons.

II-2 (3) (iii) Transaction monitoring and filtering

【Required actions for a financial institution: i】

A financial institution shall establish and maintain an appropriate control framework for monitoring transactions in accordance with the risk in order to detect transactions, etc. that would lead to detecting and reporting of suspicious transactions. Such framework would at minimum cover the followings:

(a) **Set scenarios and threshold values that reflect its own risk assessment result (Q1)**

(b) **Analyze the characteristics of the transactions for which a STR has been filed (line of business, geographic areas, etc.) and the effectiveness of the current transaction monitoring method (scenarios, threshold, etc.) (Q2)** based on the results of detection according to the criteria in (a) above and the status of STR, etc., and enhance the transaction monitoring method.

(c) **Implement appropriate risk mitigation measures according to the level of suspicion of detected transactions and trends in ML/FT risks, etc. (Q3)**

【Q1】

What are specifically required by "set scenarios and threshold values that reflect its own risk assessment result"?

【A】

When performing transaction monitoring, it is required to detect suspicious transactions by not implementing uniform scenarios and thresholds but implementing tuned ones according to the risk. For example, it is required not to implement uniform scenarios but to set different scenarios to high risk customers and low risk customers according to their risk.

It is also necessary to investigate and analyze cases of fraud, which are occurring frequently at present, and apply scenarios focusing on specific transaction patterns.

However, it is not required to tune all scenarios based on risk, and it is allowed to implement basic scenarios for all the customers and tuned scenarios for certain customers commensurate with their risk simultaneously.

Also, it takes certain period is needed to develop and evaluate the above mentioned scenarios and thresholds, therefore it is important to develop appropriate plan and consider the scenarios and thresholds, as well as periodically review their effectiveness.

【Q2】

What is required to "analyze the characteristics of submitted STR (line of business,

geographic areas, etc.) and the effectiveness of the current transaction monitoring method (scenarios, threshold values, etc.)" in particular?

【A】

FIs are required to analyze common characteristics (line of business sector and geographical areas, etc.) and transaction monitoring method (scenarios and threshold values, etc.) associated with transactions detected or submitted STRs. FIs need to identify the characteristics and transaction monitoring method that have led to more STRs, and the others that have not. It is required to evaluate the effectiveness of characteristics and whether there is room for improvement in transaction monitoring method And as for the characteristics and transaction monitoring method that have not let to more STRs, it is also required to consider their improvement and whether to remove them based on the false-positive ratio, as well as to continuously identify more effective transaction types and transaction monitoring method.

In addition, in evaluating the effectiveness of the transaction monitoring method, if an alert has not been generated for transactions in an account requested for freezing by investigative authorities, a FI shall evaluate the reason for that, and would revise the transaction monitoring method, as necessary, and continuously investigate and analyze cases of fraudulent use of products and services and fraud, which are occurring frequently at present, and review the transaction monitoring method in a timely manner as necessary.

Furthermore, it is allowed to tune alert settings in order to minimize false-positives of identical patterns (suppression). However, it is required to periodically evaluate the effectiveness of suppression logic so that suspicious transactions are not suppressed due to changes in customer attributes or those occur over time.

【Q3】

What is required to "implement appropriate risk mitigation measures according to the level of suspicion of detected transactions and trends in ML/FT risks, etc."?

【A】

In transaction monitoring, FIs are required to not only set and adjust scenarios and threshold values, but also take into account the level of suspicion of detected transactions and trends in ML/FT risks, and take appropriate risk mitigation measures, such as accelerating the time from the execution of a transaction to detection, promptly taking risk elimination measures if confirmation of fraud is obtained at the time of detection, and promptly suspending transactions and confirming with customers after detection.

For example, as an initiative to accelerate the time from the execution of a transaction to detection, it is possible to detect promptly after the execution of the transaction

depending on the status of inappropriate use of the financial institution's products and services. Here, the time from the execution of a transaction to detection may be specifically examined by each financial institution based on the characteristics of the transaction.

In addition, for example, as initiatives such as promptly taking risk elimination measures if confirmation of fraud is obtained at the time of detection and promptly suspending transactions and confirming with customers after detection, it is possible to subdivide the measures to be taken according to the level of suspicion of the detected transaction, and if confirmation of fraud is obtained, promptly take risk elimination measures to prevent fraudulent use and customer damage, such as refusal, freezing, and suspension of deposits and withdrawals, and even if confirmation of fraud is not obtained, take risk mitigation measures to prevent fraudulent use and customer damage, such as temporarily suspending transactions and confirming with customers by phone. It is possible that each financial institution will individually and specifically consider the time from detection to implementing risk mitigation measures based on the characteristics of the transaction. However, in order to promptly implement risk mitigation measures, it is important to clarify in advance the judgment criteria and the judgment process for implementing measures, such as transaction restrictions, as well as the matters to be confirmed with customers.

In order to take such appropriate risk mitigation measures, it is important to establish a framework in which FIs can promptly restrict transactions that are conducted at night or on holidays as necessary, while taking into account the hours during which operations and services are provided and the hours during which unauthorized use is common.

II-2 (3) (iii) Transaction monitoring and filtering

【Required actions for a financial institution: ii】

A financial institution shall establish and maintain an **appropriate control framework for filtering transactions (Q1)** to detect sanctioned transactions according to risk. Such framework would at minimum cover the followings:

(a)Ensure the sanction lists are up-to-date, effectively managed to screen the details of transactions (such as but not limited to: remittance destination, parties involved in transactions including their beneficial owners, import/export items), and that **the criteria for detecting sanctioned items are set appropriately according to risk (Q2)**.

(b)**Take necessary measures to comply with laws and regulations pertaining to Japan and other foreign or international sanctions and other risks (Q4)**, such as **screening a customer without delay (Q3)** when economic sanctions are designated by United Nations Security Council resolutions, etc.

【Q1】

What is specifically required by "appropriate control framework for filtering transactions"?

【A】

It is required to appropriately control the risk related to sanctioned transactions and conduct investigation according to the risk by means such as the following:

- Configure appropriate fuzzy matching algorithms to detect different spellings and register multiple names in the sanction lists when multiple alphabetical notation is expected.
- Add the followings to the original list of FIs:
  - Information obtained when conducting ongoing CDD for other customers;
  - Information obtained from transaction monitoring, transaction filtering and investigation of detected transactions;
  - Information on customers to be rejected obtained from public information; and
  - Keywords or others (e.g. high risk countries and geographies, name and organization name though not sanctioned countries, geographies or persons) to detect suspicious transactions by system and conduct in-depth investigation.

【Q2】

What are specifically required by “the criteria for detecting sanctioned items are set appropriately according to risk”?

【A】

It is required to periodically tune and appropriately configure the fuzzy matching algorithms based on own business and customers of financial institutions, etc.

【Q3】

What are specifically required by “screening a customer without delay”?

【A】

Financial institutions, etc. are required to promptly start updating their own sanction lists after the Ministry of Foreign Affairs issues the Official Gazette, and complete the screening of their existing customers.

【Q4】

What are specifically required by “take necessary measures to comply with laws and regulations pertaining to Japan and other foreign or international sanctions and other risks”?

【A】

For domestic sanctions, financial institutions, etc. are required to perform preventive measures equivalent to those for complying with laws and regulations.

For foreign sanctions, financial institutions, etc. are required to fully understand the requirement for sanction in light of the parties involved in transactions and currencies used for settlements, etc. and consider necessary measures, as well as apply preventive measures timely and appropriately, especially based on their transaction volume, business territory and business strategy according to their own risk assessment

II-2 (3) Risk mitigation

(iv) Record keeping

【Required actions for a financial institution: i】

A financial institution shall **maintain (Q2) the records necessary to implement appropriate AML/CFT measures, including evidence relevant to customers' KYC information as well as the records of transactions and communication with the customers (Q1).**

【Q1】

Please provide specific examples of "the records necessary to implement appropriate AML/CFT measures, including evidence relevant to customers' and their beneficial owners' information as well as the records of transactions and communication with the customers".

【A】

All the records necessary to ML/FT risk control for financial institutions, etc., including the identification records and transaction records required be developed by APTCP, the records related to items described in "II-2 (3) (vii)【Required actions for a financial institution: iii, a. and b.】of the Guidelines, the records on background of transaction with customers, are included.

【Q2】

Is it allowed to keep records as electromagnetic records? Is it allowed to determine the retention period according to the customer attributes or the risk?

【A】

It is allowed to keep records as electromagnetic ones.

As for retention period of the records, it is not required to establish a certain period uniformly, however, records which are required to keep a certain period by laws and regulations should be kept for the designated period.

In conclusion, Financial institutions, etc. should individually and specifically determine the format and retention period taking into account factors such as their size and characteristics, and risk of their customers based on related laws and regulations, however, they should keep records by appropriate means such as the format able to be analyzed.

II-2 (3) Risk mitigation

(v) Suspicious transaction reporting (STR)

（Main paragraph）

Suspicious transaction reporting (STR) is a legal obligation under the Criminal Proceeds Act ("APTCP"). Being "specified business operators" under the Act, financial institutions are required to fulfill their obligations to report suspicious transactions.

【Q】

What are specifically required by "financial institutions are required to fulfill their obligations to report suspicious transactions"?

【A】

It is required to verify whether there is any suspicion of money laundering or terrorist financing as set forth in Article 10 of the Act on the Punishment of Organized Crime or crimes set forth in Article 6 of the Anti-Drug Special Provisions Law with regard to transactions related to specified business affairs,(Note) and when it is so determined, promptly report the matters specified by a Cabinet Order to a competent administrative agency, pursuant to the provisions of a Cabinet Order (Article 8, paragraph 1 of the Criminal Proceeds Act ("APTCP") and Article 16 of the Order for Enforcement of APTCP).

Also, it is required not to divulge the fact that he/she is intending to make or has made a report to the customer, etc. pertaining to the said report of suspicious transactions or persons related to the customer etc. (Article 8, paragraph 3 of APTCP).

In addition, Financial institutions, etc. should investigate transactions, determine whether to file STRs and file STRs when the transaction is determined as suspicious, even if they are filing STRs based on inquiries from investigative authorities or individual requests.

(Note) Please note that the scope of the predicate offenses of the money laundering crimes were expanded by the revision of the Act on the Punishment of Organized Crime in July 2017 and violations of tax laws including the Corporation Tax Act and the Income Tax Act were included in the predicate offenses, in addition to fraud, violation of the Immigration Control law and the Stimulants Control Act.

II-2 (3) (v) Suspicious transaction reporting (STR)

【Required actions for a financial institution: i】

Establish programs for reviewing potentially suspicious transactions and determining whether STR is necessary, by comprehensively taking into account specific information available to the institution including customer attributes and circumstances of transaction and by this way **meet legal obligations and utilize the STR-related information to strengthen the financial institution's risk management (Q).**

【Q】

What are specifically required by "meet legal obligations and utilize the STR-related information to strengthen the financial institution's risk management"?

【A】

It is required not only to comply with the STR filing obligation required by APTCP and establish the framework to comply with the obligation, but also to enhance the risk control framework by utilizing the analysis of the transactions filed STRs and the information which may be reflected to the risk assessment of the Financial institutions, etc. and the scenarios and thresholds of the transaction monitoring and screening.

It is also required to manage time and streamline the process during the period from detection of suspicious activities to STR filings, review scenarios to minimize the false-positives and evaluate the effectiveness of transaction monitoring.

In detecting suspicious transactions, in addition to detection by systems, it is also critical for employees to be aware of suspicious transactions when obtaining applications from customers.

Therefore, it needs to regularly share with employees the results of the analysis of suspicious transaction reports and examples of suspicious transactions.

Employees shall detect the suspicious and unnatural transactions; it is necessary to establish a control framework that enables reporting to the head office.

In addition, it is also necessary to manage the time from detection to reporting, improve efficiency, review scenarios to reduce the false positive rate, and verify the effectiveness of transaction monitoring.

II-2 (3) (v) Suspicious transaction reporting (STR)

【Required actions for a financial institution: ii】

Establish programs for monitoring, detecting and analyzing suspicious customers and transactions (Q), utilizing IT systems/manuals fit for the business operations of the financial institution.

【Q】

What are specifically required by "Establish programs for monitoring, detecting and analyzing suspicious customers and transactions"?

【A】

It is required to establish a framework that the first and second line of defense can detect, monitor and analyze the suspicious customers and transactions or others in reference to the "Reference Cases of Suspicious Transactions", depending on the business of financial institutions, etc. including their size and characteristics. In addition, it is required to consider the implementation of appropriate system taking into account the number of customers, transaction volume or others as appropriate.

II-2 (3) (v) Suspicious transaction reporting (STR)

【Required actions for a financial institution: iii】

In determining whether STR is necessary or not, consider: customer attributes; a foreign PEP status; business activity of the customer; the countries and geographic areas involved in transactions; the nature of the transaction such as the amount and number of transactions in comparison with the customer attributes and business; and other circumstances, while taking into account the results of the National Risk Assessment and its Follow-up Report, the Reference Cases on Suspicious Transactions, FI's submitted STR cases.

【Q】

Is it required to consider all the items described in "In determining whether STR is necessary or not, consider: customer attributes; a foreign PEP status; business activity of the customer; the countries and geographic areas involved in transactions; the nature of the transaction such as the amount and number of transactions in comparison with the customer attributes and business; and other circumstances, while taking into account the results of the National Risk Assessment and its Follow-up Report, the Reference Cases on Suspicious Transactions, FI's submitted STR cases."?

【A】

As a general, it is required to consider all the items described in the Required actions (Please note that it is also required to consider the items set forth in Article 8, paragraph 2 of APTCP and Article 26 of the Regulation for Enforcement of the Act as a legal compliance).

Therefore, it needs to develop process to consider; a foreign PEPs status; customer attributes; business activity of the customer; nature of the transaction such as amount and number of transactions in light of the customer attributes and business; the countries and geographic areas involved in transactions; and other circumstances, and to develop database necessary for utilizing information, taking into account the results of the National Risk Assessment and its Follow-up Report, the Reference Cases on Suspicious Transactions, and STRs financial Institutions, etc. have filed or others.

II-2 (3) (v) Suspicious transaction reporting (STR)

【Required actions for a financial institution: iv】

Review and file a STR appropriately a transaction's nature such an ongoing transaction with an existing customer or a one-off transaction with a walk-in customer.

【Q】

What are specifically required by "Review and file a STR appropriately a transaction's nature"?

【A】

It is required to identify business relationship of the customer and the nature of the transaction and to determine whether to file STR by considering whether the transaction is suspicious taking into account the category of the transaction.

For example, when an existing customer tries to conduct a transaction at a different branch from the one the customer normally uses; at an ATM in a different area from the one where the customer normally uses the ATM, the risk is considered higher than when the customer conducts a transaction at the branch the customer normally uses. Therefore, it is considered that the reason for such a change could be carefully checked and carefully examined to ensure that it is not a suspicious transaction.

Financial institutions, etc. should identify the branch the customer regularly visit, the transaction the customer regularly perform, and the purpose of the transaction of the customer taking into account the risk when performing above mentioned measures.

II-2 (3) (v) Suspicious transaction reporting (STR)

【Required actions for a financial institution: v】

Establish a framework to promptly file a report once a transaction is determined to be suspicious.

【Q】

Please provide specific meaning of "promptly" in "establish a framework to promptly file a report"?

【A】

It is desirable to file STRs immediately after the transactions are determined to be suspicious.

For example, it is not appropriate to file suspicious transactions in a lump once a month on a fixed date of each month.

Therefore, to be considered that financial institutions, etc. "establish a framework to promptly file a report", it is required to establish a framework to file STRs immediately after the transaction is determined to be suspicious.

In addition, although it is individually considered how long the decision process should take for filing STRs taking into account necessary investigation period based on circumstances such as complexity of the transaction, it is desirable to file STRs within a month after detection.

II-2 (3) (v) Suspicious transaction reporting (STR)

【Required actions for a financial institution: vi】
Evaluate the effectiveness of risk mitigation measures for the transactions that have been reported as suspicious, and review, and modify if necessary, the mitigation measures applied to similar types of transactions.

【Q】

What are specifically required by "Evaluate the effectiveness of risk mitigation measures for the transactions that have been reported as suspicious, and review, and modify if necessary, the mitigation measures applied to similar types of transactions."?

【A】

It is required not only to appropriately comply with the filing obligation but also to evaluate ex-post-fact whether the risk mitigation measures function appropriately; additional investigations are needed to perform transactions; and STR filings are considered for similar type of transactions. And, it is required to review the risk mitigation measures applied to similar types of transactions as necessary by considering whether to modify the measures and what measures should be implemented if modifications are needed, based on the above mentioned evaluation.

II-2 (3) (v) Suspicious transaction reporting (STR)

【Required actions for a financial institution: vii】

For **customers who are determined to be at high risk**, review its customer risk rating, and apply risk mitigation measures as appropriate.

【Q】

Does “customers who are determined to be at high risk” mean that the customers who have been filed STRs should be controlled as high risk customer?

【A】

When a STR is filed, financial institutions, etc. should re-assess and update the risk level of the customer filed a STR because the property the customer received through the transaction suspected as criminal proceeds.

And it is required to apply risk mitigations measures based on the updated risk level and not required to control the customer as high risk without exception, however, it seems usual to determine the customer as high risk from the intent of the STR regime.

II-2 (3) Risk mitigation

(vi) IT systems

【Required actions for a financial institution: i】

Examine the necessity of promptly introducing an IT system according to the size and characteristics of the financial institution's business operation, and implement the items listed in ii. to v. below for the system management.

【Q】

Depending on the scale and characteristics of operations, would it be better to understand that the introduction of an IT system would not be required? Also, when is the use of IT systems required?

【A】

Regarding IT systems, each FI, etc. is required to consider the necessity of introducing IT systems and the functions of IT systems to be introduced, depending on the size and nature of their own businesses. On the other hand, depending on the actual state of FI's businesses, there is a strong need for appropriate risk control framework through the active use of IT systems.

For example, it should be noted that financial institutions where non-face-to-face transactions using the Internet, etc. dominate, or where it is difficult to verify the information only manually by employees in view of the volume of transactions, etc., may be required to have a more stringent system for obtaining customer information necessary for risk control framework and for controlling the quality of that information than financial institutions where this is not the case...

The rapid expansion of these businesses requires management's cautious judgment that ML/FT risk may be expanding beyond what was anticipated in the development of the management strategy.

II-2 (3) (vi) IT systems

【Required actions for a financial institution: ii】

The Board shall analyze the workload related to the risk control framework of ML/FT and consider the possibility of using IT systems for more efficient, effective and timely execution.

【Q】

What is the specific need for the board "when analyzing the operational burden of AML/CFT & TF related to risk control framework, and to consider the possibility of utilizing IT systems in order to conduct it more efficiently and promptly"??

【A】

The board is required to properly ascertain the burden of operations related to AML/CFT/CPF by receiving reports promptly and sufficiently from department under its responsibility, etc., and to consider the utilization of IT systems when it is judged that the use of IT systems improves effectiveness and streamlines operations, and that it can respond effectively and promptly.

II-2 (3) (vi) IT systems

【Required actions for a financial institution: iii】

In implementing IT systems as part of countermeasures against ML/FT, verify that the design and operation of the IT systems adequately respond to trends in ML/FT risks and are consistent with the risk control framework undertaken by themselves. In addition, **regularly review** and enhance, as necessary, the system.

【Q】

It says “regularly review." Who is envisaging how to implement it?

【A】

For example, a third-line internal audit department could conduct the verification from an independent standpoint or utilize outside knowledge. The entity to conduct periodic effectiveness verification should be determined on a case-by-case basis, depending on the organizational structure of each FI. Regarding the method of assurance, for example, it is conceivable to verify whether the scenarios, thresholds, etc. in the transaction monitoring system accurately capture the business and risk characteristics of each FI, taking into account the false positive detection rate and the details of false positives.

In any case, verification of the effectiveness of IT systems should be determined on an individual and granular basis according to the size and characteristics of each FI.

II-2 (3) (vi) IT systems

【Required actions for a financial institution: iv】
Evaluate the effectiveness of the IT system (Q2) by reviewing, through an independent assurance process such as **internal and external audits (Q1)**.

【Q1】

Is it better to understand that an independent verification is not to conduct both internal and external audits, but to do either?

【A】

Whether internal audits or external audits should be conducted is determined on a case-by-case basis, depending on the positioning of internal audits at each FI, etc., the organizational structure, the status of risks at each FI, etc., the abilities of internal audits, and verification issues. In addition, we may utilize the knowledge of external experts, etc. In addition, FIs may utilize the knowledge of external experts, etc.; ML/FT risk is subject to drastic changes, such as the form of occurrence and increased risks, where it is necessary to consider that it is effective to utilize external subject matter expert as needed.

【Q2】

What specific points do you envisage as verification points for the effectiveness of IT systems through internal and external audits, etc.?

【A】

For example, there are a variety of issues, including whether scenarios and threshold values in transaction monitoring system accurately grasp the nature of the businesses and risks of each FI, etc., whether matters detected in the system are accurately incorporated into the monitoring process in the businesses department and compliance/risk control department, etc., and whether the transaction filtering system is set appropriately said if there is a customary difference in the spell of the entered person name or name of place.

In any case, FIs need to determine the adequate effectiveness of their IT systems on a case-by-case basis, depending on the size and characteristics of each FI.

II-2 (3) (vi) IT systems

【Required actions for a financial institution: v】

Even in the case of outsourcing some process or using a joint system, **analyze the characteristics of its own business and accompanying risks**, and determine if additional measures are necessary.

【Q】

What is the specific expectations for "analyze the characteristics of its own business and accompanying risks"?

【A】

When outsourcing an IT system or using a joint system, FIs are required to examine whether it is appropriate to outsource or use a joint system in light of the characteristics and risks of their own transactions, and whether additional measures are required.

It is intended to alert FI and others not to implement IT systems that do not fit their own size, business model, customer base, characteristics and risks of transactions without their own review.

II-2 (3) Risk mitigation

(vii) Data governance

【Required actions for a financial institution: i】

Ensure the accuracy of customer identification records and transaction records; and **appropriately manage data as a prerequisite for the effective use of IT systems (Q2)**, by **collecting and storing accurate data and organizing it in a manner capable of analysis (Q1)**.

【Q1】

Please tell us what matters should be kept in mind when organizing data in a form that can be analyzed.

【A】

After identifying the information required for AML/CFT, it is required that the data required for system support is databased (meaning that any data can be called depending on the application).

【Q2】

Are there any demands for database management beyond the obligation of preparing and maintain KYC/CDD/EDD records and transaction records in APTCP?

【A】

As stated in this the AML/CFT Guidelines, FI, etc. requires that the records of verification and transactions be accurately recorded in compliance with relevant laws and regulations, and that data be properly managed by accurately grasping and accumulating data and organizing it in an analyzable manner, on the assumption that the IT system will be effectively utilized. Controversially, for example, where the numbers of customer and transactions are limited, there is not mandatory required to utilize IT systems. In such cases where data can be sufficiently but manually managed, etc., we do not require that KYC/CDD/EDD records and transaction records be managed by a database.

II-2 (3) (vii) Data governance

【Required actions for a financial institution: ii】

Periodically validate integrity and accuracy of the data used for IT systems (Q1) (Q2) such as customer information, customer identification records, and transaction records.

【Q1】

There is a statement that "Periodically validate integrity and accuracy of the data used for IT systems". What should we keep in mind when conducting a "validation"?

【A】

Specific methods and points to be considered for validation will be determined individually by FI according to the size and nature of the business, as well as the risks of customer.

For example, in terms of validating the data that is fed into the system, for transaction monitoring, it is required to validate that the transaction data and customer data are accurate and comprehensive, and for transaction filtering/screening, it is required to validate that the transaction data is accurate and comprehensive, respectively.

In addition, as a precondition for utilizing the data, validation is also required in terms of whether the scenarios are appropriate for transaction monitoring, and whether the lists themselves are up-to-date and appropriate for transaction filtering/screening.

【Q2】

Please tell us who assumes the validation will be conducted regarding the periodic validation of whether customer information (omit) appropriate data used in the IT system is being used...

【A】

Regarding the subject of periodic validations, validations conducted by second line such as Compliance department and Risk-Management department, and validations conducted by Internal Audit as third line of defense may be considered. Determinations will be made on an organization-by-organization basis in accordance with the size and organizational structures of each FI.

II-2 (3) (vii) Data governance

【Required actions for a financial institution: iii】

Establish an appropriate data management for collecting and storing data that can be used for risk assessments and evaluation of the effectiveness of risk mitigation measures, organizing it in a manner capable of analysis, and **making it available for submission to authorities if required (Q1)**. The data includes the items below as well as the information in the customer identification records and transaction records:

a. Number of suspicious transaction reports filed (breakdown by country/geographic area, customer attribute, etc.);
b. The numbers and contents, etc., of internal audits and training (including the numbers of employees obtained **relevant qualifications (Q2)**); and
c. Reports to the Board on ML/FT risk management, and the records of their discussions.

【Q1】

It said "making it available for submission to authorities if required". What information and periods of the data storage length do you expect to submit it?

【A】

Information to be identified and accumulated can be used for risk assessment and verification of the effectiveness of risk mitigation measure, and in addition to the information stipulated in the AML/CFT Guidelines II-2(3)(vii)【Required actions for a financial institution: iii】(a)-(c), for example: information on remittance by wire transfer (name, address, date of birth, and account number or transaction identification number in the case of individuals, name, registered address, account number or transaction identification number in the case of legal persons); the length of time between detection and filing of suspicious transaction; the length of time between the decision to its filing and actual filing date of suspicious transaction report, transactions that is determined not to be suspicious despite detection. It is assumed that this information is expected to be used for periodic and ad hoc risk assessments by financial institutions, etc., and is expected to be submitted promptly to authorities, etc., as necessary.

【Q2】

What are your assumptions about "relevant qualifications"? Does it include not only the qualifications granted by external organizations, but also internal qualifications for in-house tests?

【A】

"Relevant qualifications" in the "the numbers of employees obtained relevant qualifications" generally include qualifications granted by external organizations and Industry Association as well as internal qualifications that are encouraged to be acquired internally.

II-2(4) Considerations when making cross-border transfers and similar transactions

(i) Cross-border wire transfers and similar transactions

（Main paragraph）

(omit)

In addition, financial institutions may be required to provide adequate explanation about their ML/FT risk management and details of mitigation measures to correspondent banks and outsourced financial institutions.

【Q】

"Financial institutions may be required to provide adequate explanation about their ML/FT risk control framework and details of mitigation measures to correspondent banks and outsourced financial institutions". What exactly should we expect to explain?

【A】

For example, it is assumed that FIs disclose information to correspondents banks on the details of the overall risk control framework described in risk assessment. Financial institutions should explain the control framework of risks faced by the FI itself and the details of risk mitigation measures. Such FIs should exclude information that is inappropriate to disclose to third parties, such as internal risk management concepts and detailed procedures (e.g., customer information without customer consent to share information).

II-2 (4) (i) Cross-border wire transfers and similar transactions

【Required actions for a financial institution: i】
Evaluate the nature of foreign remittance under a risk-based structure of AML/CFT, and take **necessary measures in accordance with the risk-based approach**.

【Q】

Please tell us what matters to keep in mind when there are true originators and beneficiaries behind a customer of originators or beneficiaries of remittances abroad, etc.

【A】

If it is identified that there are true originators or beneficiaries, which is different from the originator or beneficiary, as customer of the originator or beneficiary in a cross-border wire transfer, not in the name of the requester, such as the originator's name, but in the presence of a true originator or beneficiary, the FI is required to take appropriate measures according to the relevant risk. This includes investigating the attributes of the originator or beneficiary and conducting transaction monitoring, while taking into account the real risk of the true originator or beneficiary based on a verification at the time of transactions or the like.

In case the source of funds for remittance by a customer is based on a third party's one, it is necessary to take measures in accordance with the risk, such as examining the actual business conditions and purpose of the transaction for the customer, and verifying the ML/TF risk management framework for the customer depending on the risks related to.

II-2 (4) (i) Cross-border wire transfers and similar transactions

【Required actions for a financial institution: ii】

Ensure that the ordering or intermediary financial institution informs the intermediary or beneficiary financial institution of the originator and beneficiary information **in accordance with international standards**, so that the intermediary or beneficiary institution is aware of the risks involved in the cross-border foreign remittance (Q1). Where the information is missing, the intermediary or beneficiary institution is required to take adequate measures commensurate with the risk (Q2).

【Q1】

It states "ordering or intermediary financial institution informs the intermediary or beneficiary financial institution of the originator and beneficiary information in accordance with international standards" and please provide details regarding "international standards." Also please advise on the expected information to be informed for originator and beneficiary.

【A】

The term "international standards" refers to FATF Recommendations. Pursuant to such recommendations, financial institutions shall maintain a framework to adequately inform the originator and the beneficiary information in all payment methods including SWIFT.

Originator information includes identity information or other information specified in relevant regulations, such as Article 10 of APTCP and Article 31 of Ordinance for Enforcement of the APTCP.

Beneficiary information includes (1) name, (2) if an account is used for the transaction, (3) account number or if no account is used, and (4) identification number allowing the transaction to be traced back.

【Q2】

The Guideline states that, where "the originator and the beneficiary information" is missing, "the intermediary or beneficiary institution is required to take adequate measures commensurate with the risk".
What kind of measures are envisaged?

【A】

For example, for cross boarder remittances with missing any originator or beneficiary information, the contents of the missing information may be confirmed with the

beneficiary financial institution, before the transaction is executed.

II-2 (4) (i) Cross-border wire transfers and similar transactions

【Required actions for a financial institution: iii】

When a financial institution enters into a correspondent banking arrangement in order for it to process foreign remittances, implement the measures set out in Articles 9 and 11 of APTCP and Articles 28 and 32 of the Ordinance for Enforcement of the Act. In addition, establish programs for **confirming the ML/FT risk control framework of the respondent institution** and conduct periodic reviews.

【Q】

Please advise on the methods "for confirming the ML/FT risk control framework of the respondent institution."

【A】

An example of this would be to use a questionnaire created by an organization that acts as a self-governing body for international financial transactions, which is used by various global financial institutions, or using one that was created by the financial institution itself. The intended purpose of such a questionnaire is to review ML/FT risk control framework, including any ML/FT penalties imposed or policy regarding payable-through accounts.

Based on the identification and assessed risk by the respondent institution, due diligence and risk-based mitigation measures shall be implemented. For example, if the respondent institution allows payable-through accounts, then appropriate risk-based mitigation measures must be implemented.

(Note) A correspondent account allows a third party, such as a client of a foreign financial institution, to directly use the account on their own behalf.

II-2 (4) (i) Cross-border wire transfers and similar transactions

【Required actions for a financial institution: iv】

Assess each risk of the correspondent relationship and outsourced financial institutions, etc., taking into account items, such as but not exclusively to geographic areas, customer attributes, business activities, ML/FT risk control framework, and **stance of supervision by local competent authorities (Q1)**. When there is a specific event noted and an emerging risk identified, **review the risk assessment reflecting the information obtained through the monitoring of the correspondent relationship and outsourced financial institutions, etc. (Q2)**

【Q1】

What kind of assessment is required when reviewing the "stance of supervision by local competent authorities"?

【A】

Each financial institution will be regulated by and involved with different local competent authorities. Reviewing the relevant local competent authority's supervisory guidance, contents, and frequency of sanctions is required to conduct risk assessment for each financial institution being requested.

【Q2】

What is expected of to "review the risk assessment reflecting the information obtained through the monitoring of the correspondent relationship and outsourced financial institutions, etc."?

【A】

For correspondent banks and outsourcing financial institutions, FIs are required to monitor them at a frequency appropriate to the risk assessment made when the initial relationship had been established, and review the risk assessment, taking into account the information obtained from the on-going monitoring.

Further, it is required to identify transactions with a high risk of ML/FT, and to review the risk assessment using the accumulated information to date in the event of specific events, etc., that have increased the risk to correspondent bank or outsourcing financial institution.

II-2 (4) (i) Cross-border wire transfers and similar transactions

【Required actions for a financial institution: v】

In monitoring correspondent relationships and outsourced financial institutions, etc., if the risk assessment in (iv) above indicates that **the risk is notably high, monitor them as necessary** to ensure the state of their ML/FT risk control framework.

【Q】

How should we monitor correspondents' relationships and/or outsourced financial institutions with high ML/FT risk in our risk assessment?

【A】

For such correspondent relationships and outsourced financial institutions, in addition to obtaining answers and collecting data in the prescribed questionnaire, if necessary, conduct due diligence checks to include site visits and off-site hearing focused on their ML/FT risk control framework in order to understand how the current situation should be managed. This kind of practice brings additional information, which could not have been understood from responses to the questionnaire. In addition, the scope of attendees can be expanded, such as including a specific department as the first line of defense, include an AML professional from the compliance department, or requesting more senior attendees for such meetings to allow for deep-dive monitoring on an actual situation involving ML/FT risk control framework.

II-2 (4) (i) Cross-border wire transfers and similar transactions

【Required actions for a financial institution: vi】

Do not enter into or maintain a correspondent banking arrangements, if the respondent institution is a shell bank or the respondent institution permits their accounts to be used by a shell bank.

【Q】

Please advise on the intention of the above requirement.

【A】

It is explicitly requiring FIs to not enter into or maintain a correspondent banking relationship in cases involving the respondent institution being a shell bank. FIs should not permit respondent institutions to transact with accounts used by a shell bank due to their high anonymous nature, and the high possibility of the true beneficiary or account owner being concealed, which makes this kind of relationship unfit in a correspondent banking relationship.

II-2 (4) (i) Cross-border wire transfers and similar transactions

【Required actions for a financial institution: vii】

When undertaking cross-border remittances for other financial institutions, monitor their ML/FT **risk control methodology** by questionnaire, on-site visit and/or other measures, including their customer identification/due diligence programs relating to cross-border remittances.

【Q】

For "risk control methodology" relating to cross-border remittances, apart from conducting appropriate verification at time of transactions, what are the items to be added for monitoring?

【A】

FIs must employ verification at the time of transactions and ensure record keeping, such as monitoring whether the ML/FT risk control framework is appropriately carried out. This includes checking the AML/CFT's basic processes, such as confirming whether there are no suspicious activity associated with the remittances or the amount when accepting the transaction and reviewing whether they are reasonable or not. In addition, risk-based transaction monitoring and filtering methods must be monitored.

II-2 (4) (i) Cross-border wire transfers and similar transactions

【Required actions for a financial institution: viii】

Consider as necessary, **when the originator and the beneficiary is not a direct customer (Q1)** to not only screening against the sanctions list, but also consider **conducting enhanced investigation in accordance with the risk identified (Q2)**, in cooperation with the correspondent bank and outsourcer financial institutions.

【Q1】

What types of cases are anticipated other than outgoing transaction's beneficiary and incoming transaction's originator when stating "Even when the originator and the beneficiary is not a direct customer"?

【A】

Examples of other types of cases include the following: if a FI is providing correspondent banking services to other FIs, then the originator of such transactions (a customer of the respondent bank or if the FI is acting as an intermediary institution), then the beneficiary of such incoming transactions will be in scope. Additionally, third party payment processors conducting transactions under its own name and not of the true originator's are another expected case. Further, for bulk transactions between financial institutions, on a risk-basis, there may be a case in which a framework to review the true originator will be required.

【Q2】

What can be expected when "conducting an enhanced investigation in accordance with the risk identified"?

【A】

Enhanced investigations can occur when outsourced or correspondent financial institution do not have detailed CDD information on the customers of its respondents or outsourcing institutions and it is difficult to conduct the same level of CDD that such counterparties are subject to. However, during the correspondent banking relationship, a specific transaction pattern, such as frequent transactions with countries neighboring sanctioned countries or frequent high-risk transactions, need to be identified and as part of the ongoing CDD framework. The correspondent bank is required to ask its counterparty to conduct EDD, which includes, requesting the counterparty institution to check for the purpose of transaction or actual business status. Even for transactions not of the institution's direct customer systematically monitor such transaction for any

suspicious transactions. There is a need for the outsourced or correspondent financial institution to consider the need for an EDD process through its respondent or outsourcing institution, and implement as appropriate when needed.

II-2 (4) (i) Cross-border wire transfers and similar transactions

【Required actions for a financial institution: ix】

When outsourcing cross-border remittances to other financial institutions, ensure **evaluating the nature of the cross-border remittances under the financial institution's risk-based approach**, which includes identifying, assessing, and mitigating any associated ML/FT risks.

【Q】

Please advise what is expected of "evaluating the nature of the cross-border remittances under the financial institution's risk-based approach"?

【A】

Even though cross-border wire transfers are not conducted by the FI itself and outsourced to others, it is required to reflect the fact that its customer is conducting such transactions in the customer risk assessment. Based on the customer risk assessment, a risk-based CDD needs to be conducted to ensure its own ML/FT risk identification, assessment, and mitigation measures are in place with respect to such customers.

II-2(4) Considerations when making cross-border transfers and similar transactions (ii) Financing and extending credit involving trade based finance

（Main paragraph）

Compared to domestic transactions, it is easy to abuse trade finance for illicit purposes due to the fact that it is more difficult to verify the actual location of import/export transactions, and to transfer the proceeds of crime by disguising import/export transactions or paying an additional/different amount to the actual transaction/unit price. In addition, there is a risk that the goods could be used for a dual purpose specifically for the trade of materials for military use or illegal drugs through fraudulent statements of import and export.

A financial institution needs to identify, assess, and mitigate specific risks appropriately by recognizing that **financing and extending credit for import/export transactions** pose such risks.

【Q】

What are the expected cases when referring to "financing and extending credit for import/export transactions"?

【A】

These terms includes providing the following during the course of a trade transaction: fulfillment of the guarantee in case of default, performance guarantee, provide financing, negotiation of the draft/letters of credit, issuing letters of credit, and confirmation on letters of credit.

For a straightforward cross-border payment guidance for import and exports, please refer to the "Guidelines II-2(4)(i) Cross-border wire transfers and similar transactions."

II-2 (4) (ii) Financing and extending credit involving trade based finance

【Required actions for a financial institution: i】

Identify, assess and mitigate the risks associated with the financing and extending credit related to import/export transactions, etc.; not only the risks of the country/region involved in the import/export transaction, but also the risks of the commodities to be traded, the content of the contract, the transportation route, the vessel to be used, etc., and the risks of the parties involved in the transaction, etc. (including the beneficial owner) shall be taken into consideration.(Q1, 2)

【Q1】

Regarding “identify, assess and mitigate the risks associated with the financing and extending credit related to import/export transactions, etc.; not only the risks of the country/region involved in the import/export transaction, but also the risks of the commodities to be traded, the content of the contract, the transportation route, the vessel to be used, etc., and the risks of the parties involved in the transaction, etc. (including the beneficial owner) shall be taken into consideration”, what kind of measures are required specifically?

【A】

With regard to identify, assess and mitigate the risks associated with the financing and extending credit related import/export transaction, etc., it requires to consider not only the countries and regions involved in the transaction but also risks to the entire transaction.

As for "commodities", it is necessary to confirm whether they can be used for military purposes.

As for transportation route, it is necessary to consider necessary items from the perspective of whether or not they will be used for bridging a country subject to sanctions. Therefore, it is necessary to confirm the ports of departure, ports of call, and transit points based on export-import related documents. Especially, if the goods pass through the vicinity of sanctioned countries, it may be possible to confirm the content of the sanctions from the viewpoint of whether the sanctioned country is involved in transactions, and whether it has passed the sanctioned country or region.

If a business partner uses a trade intermediary operator, it is necessary to take necessary measures, such as confirming the true exporter through the relevant operator.

As for the vessel to be used, it is possible that necessary matters should be considered from the viewpoint of whether the vessels or the owners and operators of the vessels are not subject to sanctions.

As for the parties involved in the transaction, it is possible to consider the parties involved in identifying and assessing risks, such as financing and extending credit related to import/export transactions. If a beneficial owner exists for that party, that beneficial owner will also be considered.

However, this does not mean that financial institutions are required to conduct customer identification procedures and customer risk assessment for the customer of customer, so called KYCC (Know Your Customer's Customer).

【Q2】

What is specifically required by mitigating the risks associated with financing and extending credit related to import/export transactions, etc.?

【A】

As described in Q1 above, it is necessary to mitigate risks through CDD, transaction monitoring, transaction filtering, etc. on a risk basis, taking into account the risks of transactions as a whole. It is necessary for each financial institution to consider specific measures to mitigate risks on a risk basis.

For example, in transaction monitoring, it would be desirable to ensure the appropriate detection of high-risk transactions by identifying key indicators for understanding risk, and by listing products considered high-risk, such as dual-use products and customer attributes considered high-risk, such as customers who have a record of filing STR from the viewpoint of risks related to financing and extending credit related to import/export transactions, etc.

For example, it would be desirable to confirm whether or not there is a difference between product values and market values, and if there is a difference without grounds, it is desirable to understand the actual situation further, such as by obtaining additional information.

It is possible to screen documents against the sanctions list, etc. not only at the time of document receipt, but also at the time of amendment and at the time of transaction execution. Such re-screening control includes the following cases: when the type of commodity being shipped appears inconsistent with the exporter or importer's regular business activities and an unusual transaction pattern is observed at the time of document receipt where there are inconsistencies in information contained in trade documents and financial flows, such as names, companies, addresses, final destination, etc.; there is a certain time difference between the time of document receipt and the time of transaction execution; or when trade documents, etc. are amended between the time of document receipt and the time of transaction execution.

In addition, it is useful to examine the necessity of introducing an IT system/database for the management of financing and extending credit for import/export transactions, etc., depending on the scale and characteristics of the business.

III-1 Formulation, implementation, evaluation, and review of AML/CFT policies, procedures and programs (PDCA)

（Main paragraph）

Financial institutions are required to prepare **AML/CFT policies, procedures, and programs** and disseminate them throughout the organization in order to establish an effective ML/FT risk control framework and to function effectively.

Such policies, procedures, and programs must be designed to ensure the effectiveness of the AML/CFT measures commensurate with the risks the financial institution faces and clearly define the sequential processes of identifying, assessing, and mitigating the risks, taking into account the institution's size and characteristics.

(Omitted)

【Q】

What is "programs" in "AML/CFT policies, procedures and programs ".

【A】

A series of programs, including internal control framework, audit, and training are designed to enhance the effectiveness of AML/CFT measures at each financial institution. For example, it there is a gap between the "Required actions for a financial institution" in the Guidelines and the current situation of each financial institution, an action plan with a deadline for completion to eliminate the gap is also included.

As long as "programs" are effective based on the above intent, it is permissible to prepare them together with "policies and procedures" as attached documents. However, it is assumed that "policies, procedures, and programs" will be established in different documents.

III-1 Formulation, implementation, evaluation, and review of AML/CFT policies, procedures and programs (PDCA)

【Required actions for a financial institution: i】

Formulate AML/CFT policies, procedures and programs **considering the risks in light of the business sector of the institution and geographic area in which it operates as well as the trend of ML/FT**, and apply specific approaches and practices of customer acceptance policies, CDD, record-keeping and other processes in a consistent manner across the organization.

【Q】

Regarding "considering the risks in light of the business sector of the institution and geographic area in which it operates as well as the trend of ML/FT", what kind of measures are required specifically?

【A】

In formulating AML policies, procedures and programs, it is necessary to consider not only risk assessment that comprehensively and concretely examines products and services, countries and geographic areas, transaction types, customer attributes, but also risks in light of the business sector of the institution and geographic area in which it operates as well as the trend of ML/FT.

III-1 Formulation, implementation, evaluation, and review of AML/CFT policies, procedures and programs (PDCA)

【Required actions for a financial institution: ii】

Conduct ongoing evaluation on effectiveness of the policies, procedures, and programs for identifying, assessing, and mitigating risks, taking into account the results of monitoring of each division and branch.

【Q】

Regarding "conduct ongoing evaluation on effectiveness of the policies, procedures, and programs for identifying, assessing, and mitigating risks, taking into account the results of monitoring of each division and branch", what kind of measures are required specifically?

【A】

Policies, procedures, and programs for identifying, assessing, and mitigating risks, it is necessary for financial institutions to appropriately comply with such policies, procedures, and programs, as well as to exercise an appropriate check-and balance function by the department in charge. In the event that changes in risk trends are identified or operational issues are identified, it is necessary to examine in order to ensure effectiveness constantly. Therefore, it is not enough to formulate policies, procedures, and programs by itself, and it is necessary to continuously implement verification and improvement to ensure effectiveness on an organizational bases.

III-1 Formulation, implementation, evaluation, and review of AML/CFT policies, procedures and programs (PDCA)

【Required actions for a financial institution: iii】

Consider the need to improve risk mitigation measures, including whether or not they offer such product/services, or to implement further measures, depending on the risk appetite of a financial institution and the impact on it, etc., by assessing **residual risks after risk mitigation measures have been taken.**

【Q】

Regarding “residual risks after risk mitigation measures have been taken”, how it should be considered?

【A】

It is necessary to minimize residual risks as much as possible within the risk tolerance of each financial institution through risk mitigation measures, and it is considered to be difficult to maintain these products and services with high residual risks. In order to improve risk mitigation measures from high risk to medium risk and from medium risk to low risk, while assuming that the residual risk will not be zero, it is necessary to periodically examine whether it is possible to mitigate risks by, for example, improving thresholds and scenarios based on the results of analysis of suspicious transaction reports, and to consider including the Board..

Ordinary deposit account transactions are one example of the risk remaining even after risk mitigation measures are taken. This is the case where customers who are identified as anti-social forces after the commencement of transactions are allowed to maintain their accounts as minimum living accounts while maintaining strict control until the transactions are terminated.

III-1 Formulation, implementation, evaluation, and review of AML/CFT policies, procedures and programs (PDCA)

【Required actions for a financial institution: iv】

Have the control division and internal audit division evaluate the effectiveness of the risk control framework (Q2), taking into account internal information, whistle-blowing reports and questions from employees (Q1).

【Q1】

Regarding “taking into account internal information, whistle-blowing reports and questions from employees", what should be in mind when evaluate the effectiveness of the risk control framework?

【A】

Control division and internal audit division are required to evaluate the effectiveness and risk control framework by setting check items in consideration of various circumstances in order to conduct effective verification based on specific circumstances.

Information such as internal information, whistle-blowing reports and questions from employees are useful information for evaluating whether the risk control framework is effective (whether or not it is possible and easy to implement for the first line) (for example, regarding matters that received many questions, the rule may be difficult to understand, so it is possible to review the description method).

However, this information is merely an example, and the control division and internal audit division need to take into consideration various circumstances and use it as an opportunity to evaluate the effectiveness of the risk control framework.

【Q2】

Regarding "the control division and internal audit division evaluate the effectiveness of the risk control framework”, what is specific items to be evaluated?

【A】

For example, based on internal information, whistle-blowing reports and questions from employees, various matters can be considered, such as confirming the status of compliance with AML/CFT policies, procedures and programs on the first line, analyzing the status of STR, and evaluating the effectiveness of existing procedures related to the types of transactions frequently filled.

In any case, evaluating the effectiveness of ML/FT risk control framework should be evaluated individually according to the size and characteristics of each financial

institution.

III-1 Formulation, implementation, evaluation, and review of AML/CFT policies, procedures and programs (PDCA)

【Required actions for a financial institution: v】

If, as the result of the aforementioned evaluation of effectiveness, possibilities of further improvements are identified, **enhance the policies, procedures, programs, and risk control framework, for the identification, assessment and mitigation of risks**.

【Q】

Regarding "enhance the policies, procedures, programs, and risk management, for the identification, assessment and mitigation of risks", in cases where the effectiveness of the risk control framework has been evaluated and there is room for further improvement, is it sufficient to review only risk control framework in which problems have been identified as necessary?

【A】

If a problem is found in the effectiveness of the risk control framework, it is necessary to analyze the cause of the problem and take appropriate measures for improvement. However, it is also necessary to review the identification, assessment and mitigation of risks, which are basis of the risk control framework, and of course, it is also necessary to review the methods.

III-2 Involvement and understanding of the Board

（Main paragraph）

(omit)

Furthermore, “tone at the top” is critical to increase the awareness of AML/CFT measures among all executives and employees including the business divisions. The Board must therefore have a keen awareness of AML/CFT based on proper understanding of the risks mentioned above, and demonstrate its commitment and clear policy, to promote enhancement of measures throughout the organization from the top down.

In light of this, **the Board of financial institutions, etc., shall take leading role** in promote the enhancement of their own countermeasures against ML/FT.

【Q】

Can “take leading role by the Board” be understood to, for example, the involvement of the director in charge of AML/CFT in the process of risk assessment and in the AML Committee/Compliance Committees etc. held regularly within his/her organizational unit?

【A】

One involvement of the Board is to participate in and discuss meetings such as question, but the manner in which the Board is involved is not limited to this.

The Board is required to properly recognize that ML/FT risk may pose a serious management risk. The Board of Directors, etc. is required to position AML/CFT as one of the key issues in management strategy, etc. and to establish a cross-organizational framework for the Board's liabilities and implement strategic recruitment of human resources (including IT systems and data analysis specialists, etc.), training and resource allocation, etc.

III-2 Involvement and understanding of the Board

【Required actions for a financial institution: i】

Recognize AML/CFT as one of the most important strategic issues.

【Q】

Regarding “recognize AML/CFT as one of the most important strategic issues”, what is specifically required?

【A】

As one of the most important strategic issues, AML/CFT must be disseminated within and outside the organization to take various measures to ensure their effectiveness. It is necessary for the Board to confirm that organizational actions have been secured while understanding that these various measures have been appropriately implemented and that constant reviews have been implemented.

III-2 Involvement and understanding of the Board

【Required actions for a financial institution: ii】
Appoint an executive (Q1) responsible for AML/CFT measures of the institution (Q2), granting the authority necessary to fulfill the responsibilities.

【Q1】

Please tell us about the definition of "executive" in this item.

【A】

The term "executive" as used in the AML/CFT Guidelines III-2【Required actions for a financial institution: ii】means a director or any other person in a position equivalent thereto under the Companies Act (even a person who is not a director under the Companies Act, such as an executive director, may be regarded as an "executive"), and is required to be a person who has the right to speak and vote at a meeting body that is authorized to decide the policy of an organization, such as the Management Committee.

In any case, financial institutions are required to appoint a person who is responsible for AML/CFT in accordance with its size and organizational structure, and to grant such person the necessary authority to fulfill his/her duties.

【Q2】

Regarding "appoint an executive responsible for AML/CFT measures of the institution", is it better to clarify the executive in charge of AML/CFT organizationally, taking into account the fact that the executive responsible for risk measures is made known to the first line?

【A】

As stated in the main text of the AML/CFT Guidelines, it is necessary to appoint a person responsible for AML/CFT from among the executives, to grant the authority necessary to fulfill the duties, etc., to provide the relevant executives with the necessary information in a timely and appropriate manner, and to establish an control framework in which the relevant executives can explain AML/CFT in financial institutions. internally and externally.

It is also desirable that persons responsible for AML/CFT be made known both inside and outside the organization by including them in organizational charts and in publicly available documents such as disclosure publications and annual reports.

III-2 Involvement and understanding of the Board

【Required actions for a financial institution: iii】

Establish programs by which necessary information is provided to the executive responsible for AML/CFT in a timely and appropriate manner so that the executive can explain the financial institution's AML/CFT measures to internal and external stakeholders.

【Q】

Regarding "establish programs by which necessary information is provided to the executive responsible for AML/CFT in a timely and appropriate manner so that the executive can explain the financial institution's AML/CFT measures to internal and external stakeholders", what points are required to bear in mind specifically?

【A】

The executive responsible for AML/CFT must, at a minimum, be able to adequately explain he/she is asked the content of cross-organizational AML/CFT, their own AML/CFT Report, and the risks they face. In addition, the executive must constantly endeavor to ascertain all other AML/CFT.

The content of AML/CFT may also be described in external public documents such as disclosure publications and annual reports.

III-2 Involvement and understanding of the Board

【Required actions for a financial institution: iv】

In view of the importance of AML/CFT, allocate adequate resources such as personnel with expertise and sufficient budget to the division responsible for AML/CFT.

【Q】

Regarding "in view of the importance of AML/CFT, allocate adequate resources such as personnel with expertise and sufficient budget to the division responsible for AML/CFT", what points are required to bear in mind specifically?

【A】

Division responsible for AML/CFT are required not only to properly allocate expertized personnel and allocate the necessary budgets, but also to enhance AML/CFT of the entire organization by considering human resources and human resource allocation also in other divisions for financial institutions to allocate resources to ensure that their measures to provide AML/CFT are sustainable and enhanced.

In addition, it is possible to ensure that an appraisal and remuneration system appropriately reflects the compliance records and contributions of executives and employees to AML/CFT measures, as necessary.

III-2 Involvement and understanding of the Board

【Required actions for a financial institution: v】
Establish programs for coordination between the executives and divisions involved in AML/CFT.

【Q】

Regarding "establish programs for coordination between the executives and divisions involved in AML/CFT", what points are required to bear in mind specifically?

【A】

Since AML/CFT require company-wide efforts, it is effective to prepare in advance a framework to smoothly resolve conflicts of interest that arise between executives and divisions, such as by establishing a meeting body to regularly exchange information and assigning contact officers to relevant executives and division heads.

III-2 Involvement and understanding of the Board

【Required actions for a financial institution: vi】

Ensure that the Board approves the design and review of policies, procedures, and plans for countermeasures against ML/FT, and **the Board takes the initiative in the implementation** of such policies, procedures, and plans by receiving reports on a regular and ad hoc basis and holding discussions as necessary.

【Q】

Regarding “the Board takes the initiative in the implementation”, what is required specifically?

【A】

"The Board takes the initiative in the implementation" does not require the Board to implement all measures. In implementing AML/CFT on a company-wide basis, it is important for the Board to appropriately implement support for division that actually implement various measures, such as the framework of necessary collaboration, authority of division, and allocation of human resources, so that the measures can be implemented smoothly and efficiently.

As part of this effort, it is clear that the Board should take appropriate measures when approval and discussions are necessary.

III-2 Involvement and understanding of the Board

【Required actions for a financial institution: vii】
Ensure that the Board participates or is otherwise proactively involved in AML/CFT training for the Board and employees.

【Q】

Regarding "ensure that the Board participates or is otherwise proactively involved in AML/CFT training for the Board and employees", what points are required to bear in mind specifically?

【A】

In addition to the participation of the Board in training on AML/CFT for employees to gain wide range of knowledge, it is important to provide more training opportunities for the Board, such as conducting training on AML/CFT for the Board and disseminating this within the company.

III-3 The Board and control: three lines of defense

（Main paragraph）

In the following sections, the functions in the ML/FT risk control framework by financial institutions are defined under the concept of three lines of defense and required actions are provided. Each financial institution may **formulate its risk control framework** under a different model, **including outsourcing**, depending on the characteristics of its business operations. In such instances, those financial institutions are required to design programs that achieve the same level of effectiveness that is required with the required actions.

【Q】

Regarding "(omit) formulate its risk control framework including outsourcing", what points are required to bear in mind specifically?

【A】

In the event that the outsourcing contractor performs some of identification and verification at the time of transactions and CDD operations, the outsourced financial institution is responsible for CDD. For this reason, for example, it is necessary to position this outsourced financial institution as the first line, and the second line will conduct the necessary checks and supports, and carry out the necessary document management under the responsibility of the outsourced financial institution. In this case, the third line will audit whether the outsourcing contractor is checking and supporting appropriately at the second line.

In addition, in the event personal information is transferred to or received from outsourcing contractor, it is necessary to bear in mind that an agreement on the sharing of personal information has been obtained in advance with the outsourcing contractor and that the outsourcing contractor has been confirmed to be a party that has no problems with information security or the conclusion of confidentiality obligation agreements.

III-3 The Board and control: three lines of defense

(1) First line of defense

【Required actions for a financial institution: i】

Ensure that all employees belonging to the first line have sufficient understanding of the AML/CFT policies, procedures, and programs applicable to their division and duties, and properly implement the mitigation measures commensurate with the risks.

【Q】

Regarding "ensure that all employees belonging to the first line have sufficient understanding of the AML/CFT policies, procedures, and programs applicable to their division and duties, and properly implement the mitigation measures commensurate with the risks", what points are required to bear in mind specifically?

【A】

All employees on the first line face direct customer, and are required to fully understand the policies, procedures, execution plan related to AML/CFT and implement risk mitigation measure in accordance with these policies. Accordingly, it is necessary to ensure that all employees on the first line have the opportunity to acquire the necessary knowledge in the course of their duties and that appropriate measures are implemented.

The following flow is desirable as a best practice. First, it is desirable for the second line to conduct autonomously and in accordance with the rules stipulated in the second line, risk assessment of products and services, transactions types, countries and geographic areas, and customer bases, and customer risk assessment as well as mitigation measures.

In addition, the second line may determine the appropriateness of risk assessment by the first line as a part of quality control operations and re-examine risk mitigation measures in accordance with the risk. In addition, it is desirable that the third line may implement internal audits from an independent stand point while managing the PDCA cycle and develop a system to exercise a check-and –balance function. Therefore, the first line must fully understand the risks faced by the financial institution and properly implement the risk mitigation measures stipulated by the second line. Also, the first line must have a control framework in place to accurately communicate to the second line about the risk awareness of the first line.

III-3 (1) First line of defense

【Required actions for a financial institution: ii】

Provide a clear and easy-to-understand description for employees of their obligations and instructions in the AML/CFT policies, procedures, and programs, and communicate them with all employees of the first line.

【Q】

Regarding "provide a clear and easy-to-understand description for employees of their obligations and instructions in the AML/CFT policies, procedures, and programs, and communicate them with all employees of the first line", what points are required to bear in mind specifically?

【A】

"Provide a clear and easy-to-understand description for employees of their obligations and instructions in the AML/CFT policies, procedures, and programs, and communicate them with all employees of the first line" means not only to provide clear and easy to understand explanations, but also to ensure that all employees in the first line are aware of their own responsibilities and understand them to extent that they can able to take measures appropriately, and to confirm the level of understanding as necessary.

III-3 The Board and control: three lines of defense

(2) Second line of defense

【Required actions for a financial institution: i】

Monitor independently whether the ML/FT risk control framework is functioning effectively, for example, by checking compliance by the first line with AML/CFT policies, procedures and programs, and evaluating the effectiveness of mitigation measures implemented by the first line.(Q1, 2)

【Q1】

What are the specific requirements for the second line concerning "compliance by the first line with AML/CFT policies, procedures and programs, and evaluating the effectiveness of mitigation measures implemented by the first line"?

【A】

The second line is required to regularly evaluate the status of compliance with the first line's procedures and the effectiveness of risk mitigation measure, considering not only the compliance with laws and regulations, but also the risks faced by matters recognized through analyses of suspicious transaction report and other means, from the viewpoint of whether ML/FT risk management is functioning effectively, for operations of identification and verification at the time of transactions and identification and verification at the time of transactions records creation and keeping operations handled by the first line.

In particular, when conducting identification and verification at the time of transactions operations on a non-face-to-face basis, the risk is higher than when on a face-to-face basis, and therefore control framework in accordance with the risk is required. If there are deficiencies in identification and verification at the time of transactions operations, and the accuracy of customer information such as matters specified by the employee is not ensured, not only may there be violations of laws and regulations, but also customer information required for risk management is unavailable. In other words, accurate understanding of customer information is a prerequisite for ML/FT risk management, and in the absence of this, it is not able to identify and assess risks faced by financial institutions, and to take risk mitigation measure commensurate with their own risks, such as ongoing CDD and transaction monitoring based on customer risk assessment.

For this reason, the second line is required to regularly confirm and evaluate the status of compliance with the first line procedures and the effectiveness of risk mitigation measures.

【Q2】

What are the specific points to note concerning monitor independently whether the ML/FT risk control framework is functioning effectively?

【A】

For example, it is possible to establish, as appropriate, a department solely dedicated to the implementation of AML/CFT measures, taking account of the institution's size, characteristics, and business operations and other factors, and undergo a review by an external expert, as appropriate. However, since the organizational structure and specific monitoring methods vary depending on the size, characteristics, and business profile of the financial institution, it is necessary for each financial institution to consider appropriate measures based on its own size, characteristics, and business profile.

III-3 (2) Second line of defense

【Required actions for a financial institution: ii】

Provide sufficient support to the first line, for example, by providing information and responding to questions relating to ML/FT and by advising on specific measures.

【Q】

Regarding "provide sufficient support", what points are required specifically?

【A】

Providing support to the first line by the second line is not limited to providing information and responding to questions. For example, support by the second line is provided from behind the first line by providing advice that fully demonstrates its expertise and through dialogue with external experts and authorities in responding to individual case. As a department in charge, the second line needs to provide support for the first line to ensure consistency with AML/CFT on a company-wide basis and to implement responses with maximum consideration to facilitating transactions.

III-3 (2) Second line of defense

【Required actions for a financial institution: iii】

Clarify the roles and responsibilities of the division in charge of AML/CFT and all other divisions involved in AML/CFT, and share the understanding of the roles and responsibilities of each division. In addition, establish a collaborative environment between the division in charge of AML/CFT and other divisions, and **ensure close communication and coordination**.

【Q】

Regarding "ensure close communication and coordination", what points are required specifically?

【A】

In promoting company-wide AML/CFT, it is necessary to clarify the roles and responsibility of the division in charge and related divisions, and to develop a system for close information sharing, collaboration, and cooperation.

To do this, each division must be able to access the information managed by other divisions in a timely and appropriate manner.

III-3 (2) Second line of defense

【Required actions for a financial institution: iv】

Allocate employees with sufficient knowledge and expertise of AML/CFT to control divisions.

【Q】

Regarding "allocate employees with sufficient knowledge and expertise", what points are required to bear in mind specifically?

【A】

In implementing company-wide AML/CFT, control divisions are required to assign employee with knowledge and expertise. However, it is not enough to assign employees who are certified relevant AML/CFT qualifications, and it is important to determine expertise while continuing education and training in consideration of practical experience.

III-3 The Board and control: three lines of defense

(3) Third line of defense

【Required actions for a financial institution: i】

Formulate an audit plan that includes the following items in audit scope and conduct audits adequately:

a. Appropriateness of the AML/CFT policies, procedures, and programs;

b. The expertise and competency of employees in charge of implementing such policies, procedures, and programs;

c. The effectiveness of employee training;

d. The status of detection of unusual transactions in the business division;

e. Operating status of IT systems including the effectiveness of detection standards; and

f. The status of the implementation of risk mitigation measures for detected transactions and of STR.

【Q】

Regarding "Formulate an audit plan that includes the following items in audit scope and conduct audits adequately", what points are required to bear in mind specifically?

【A】

In the third line, it is important to confirm from an independent standpoint whether AML/CFT established by the second line are effectively implemented on the first and second lines and to report to management. Therefore, items a. to f. in the above 【Required actions for a financial institution: i】 should be included as a minimum in the audit plan, and it is necessary to consider the additional items that are necessary to confirm the effectiveness of the AML/CFT and to conduct audits appropriately.

III-3 (3) Third line of defense

【Required actions for a financial institution: ii】
Ensure that the scope, frequency and approaches of audits are appropriate in light of the ML/FT risks being faced.

【Q】

Regarding “ensure that the scope, frequency and approaches of audits are appropriate in light of the ML/FT risks being faced”, what points are required to bear in mind?

【A】

For example, in examining transactions, it is necessary to assess ML/FT risks faced by oneself and set appropriate verification methods, considering that the volume of transactions is increasing in countries and geographic areas where the volume of transactions is increasing. Therefore, it is necessary to analyze risks and conduct comprehensive surveys as necessary, rather than conducting surveys by sampling in all areas.

In addition, when setting the verification methods based on risks faced by oneself, it is considered that not only the risk assessment performed by the second line but also the risk assessment may be performed by the third line as necessary.

III-3 (3) Third line of defense

【Required actions for a financial institution: iii】

Take necessary measures for business operations other than those assessed to have high risk. For example, instead of uniformly excluding such operations from the audit scope, conduct audits by adjusting the frequency and depth.

【Q】

Regarding "take necessary measures for business operations other than those assessed to have high risk. For example, instead of uniformly excluding such operations from the audit scope, conduct audits by adjusting the frequency and depth", what points are required specifically?

【A】

The risk-based approach is required to be applied to audits conducted by the third line. However, in selecting specific audit items, it is not a risk-based approach to uniformly exclude those items that are determined to have low risk based only on the level of risk.

It is clear that for items with low risk that have not been audit in the past, it is necessary to conduct audits on a sample basis by adjusting the depth.

III-3 (3) Third line of defense

【Required actions for a financial institution: iv】

Report the results of the internal audits conducted by the internal audit division to the corporate auditors and the Board, and follow up on the audit results and advise on improvements.

【Q】

Regarding "report the results of the internal audits conducted by the internal audit division to the corporate auditors and the Board, and follow up on the audit results and advise on improvements", what does it mean?

【A】

Responsibilities of internal audit division include not only conducting audits and reporting the results to corporate auditors and the Board, but also clarify that providing follow up on the audit results and advice on improvements are included.

III-3 (3) Third line of defense

【Required actions for a financial institution: v】
Allocate employees with the sufficient knowledge and expertise of AML/CFT to the internal audit division.

【Q】

Regarding "allocate employees with the sufficient knowledge and expertise of AML/CFT to the internal audit division", what does it mean?

【A】

Internal audit division requires to allocate employees with sufficient knowledge and expertise. However, it is not enough to assign employees with qualifications related to AML/CFT. It is important to conduct continuous education and training in addition to determining expertise in consideration of practical experience.

III-3 The Board and control: three lines of defense

(4) Management of Outsourcing of ML/FT Risk Management

【Required actions for a financial institution: i】

When outsourcing ML/FT risk management (Q1), verify the control framework of the outsourcing contractor from the viewpoint of achieving the same level of effectiveness that is required with the "required actions." (Q2, 3)

【Q1】

Regarding “when outsourcing ML/FT risk management”, what kind of operations should be outsourced?

【A】

Depending on the items, each financial institution may outsource ML/FT risk management based on the characteristics of its business.

Any outsourcing by a financial institution should not necessarily be subject to the requirements of this section. The outsourcing of even a part of ML/FT risk management by a financial institution should be considered subject to the requirements of this section.

It is necessary for each financial institution to consider what kind of operations should be outsourced and what measures should be taken to comply with the requirements in this section. In cases where the ML/FT risk management framework of an outsourcing contractor is deemed to have an impact on the robustness of its ML/FT risk management framework, it is necessary to take into account the characteristics of the outsourced operations and the role of the outsourcing contractor in the outsourced operations when conducting reviews of the ML/FT risk management framework of the outsourcing contractor.

【Q2】

Specifically, what kind of points are required to be considered regarding "verify the control framework of the outsource from the viewpoint of achieving the same level of effectiveness that is required with the "required actions""?

【A】

Each financial institution develops its ML/FT risk management framework so that it can respond to the matters described in the "required actions" of the Guidelines. Even if operations related to ML/FT risk management are outsourced, the outsourcing financial institution assumes the responsibility for ML/FT risk management related to the outsourced operations. Therefore, with respect to outsourced ML/FT risk management

operations, it is important for the outsourcer financial institution to verify that the outsourcee has a control framework that enables the outsourcee to respond to the matters described in the "required actions" of the Guidelines, that is, to achieve the same level of effectiveness that is required with the "required actions."

As described in Q1 above, each financial institution needs to consider what kind of operations should be outsourced and what measures should be taken to comply with the requirements in this section. Regarding verification methods, various methods may be used depending on the characteristics of the operations for which outsourcing is being considered and the role played by the outsourcing contractor in the operations, such as checking the results of the performance of the outsourced operations after the fact, requiring the outsourcing contractor to implement reliable operations based on the contract with the outsourcing contractor, and listening to the policies and the operation execution framework of the outsourcing contractor in detail using questionnaires, etc. Therefore, it is important for each financial institution to consider the method and timing of verification, taking into account the characteristics of the operation for which outsourcing is being considered and the role played by the outsourcing contractor in the operation.

【Q3】

What points should be kept in mind when reviewing the effectiveness of ML/FT risk management by external experts?

【A】

A financial institution is responsible for its ML/FT risk management even when its ML/FT risk management framework is reviewed by external experts. Therefore, it is important for each financial institution to pay attention to the appropriateness of external experts.

For example, prior to appointing external experts, the adequacy of the external experts shall be reported to and approved by the Board when receiving reviews by external experts for the review and assessment of the risk management framework for ML/FT. In addition, the internal audit department shall conduct post-evaluation of the appropriateness and capability of external experts, etc. as necessary. In any case, it is important for each financial institution to consider specific measures based on the scope of the review and the roles of external experts.

III-4 Group-wide risk control framework

（Main paragraph）

A **financial institution that forms a financial group (Q1)** is required to formulate group-wide AML/CFT policies, procedures and programs, and apply them consistently across the group, taking into account the differences in the business sectors of group entities, and the countries and geographic areas in which they operate

(omit)

Therefore, a **financial group that operates through overseas offices (Q2)** is required to establish risk control framework consistently applied on a group basis and exercise appropriate oversight of the business operators within the group, taking into account such differences as well as the practices of other financial groups that are operating globally. This is particularly relevant for financial groups in which their overseas operations represent a large proportion of their business or those which recognize the operations as strategically important, given rapidly increasing calls for stricter AML/CFT measures.

Japanese offices of foreign financial groups (Q3) are required to fulfill accountability to the Japanese authorities and other stakeholders for their ML/FT risk control framework of the group as a whole, and the status of transactions with Japanese financial institutions including correspondent banking relationships.

【Q1】

Regarding the group-wide and global-wide development of risk control framework, can the scope of the group companies to be managed and the level required for each company be based on a case-by-case basis according to the business type of each financial institution?

【A】

The scope of the Group needs to be determined individually according to the risks of each group company in light of the intent of the AML/CFT Guidelines requiring the establishment of group-wide risk control framework, and is not determined mechanically by the percentage of ownership of (consolidated) subsidiaries or equity-method affiliates.

The level required for each business operator forming a group also needs to be determined individually according to the risk of each group company. These judgments need to be approved by department responsible for group management at head office, which oversees the entire group.

【Q2】

What are assumed about "overseas offices"? Are overseas subsidiaries, branch offices, and representative offices included in "overseas offices"?

【A】

"Overseas offices" are generally considered to include overseas subsidiaries, branch offices, and representative offices. In any case, it is necessary to make specific judgments individually according to risks, etc. by considering the nature of the operations of each overseas offices. For example, the risks by considering the nature of operations differ between overseas subsidiaries and branches that conduct business with the approval of local authorities, and representative offices that do not conduct business, but are for the purpose of collecting information.

【Q3】

If a reasonable measures have already been implemented, mainly by the foreign head office of the foreign financial group, and if it is linked to control framework of AML/CFT in the Japanese offices, would it be possible to implement these measures at the Japanese offices while effectively utilizing control framework as a group?

【A】

If an appropriate measures are implemented in accordance with the purpose of this the AML/CFT Guidelines, such understanding is acceptable.

III-4 Group-wide risk control framework

【Required actions for a financial institution: i】

Formulate group-wide AML/CFT policies, procedures, and programs consistently applied across the group, and **implement the customer acceptance policy, specific CDD measures and record-keeping standard in a consistent manner throughout the entire group**, in consideration of its business categories and geographic areas in which it operates.

【Q】

Regarding "implement (omit) in a consistent manner throughout the entire group", what points are required to bear in mind specifically?

【A】

In case where financial institutions form a group, AML/CFT policies, procedures, and programs applied, and the group considers that the group is responding as a single company, and requires implementing in a consistent manner throughout the entire group. Accordingly, it is necessary for companies within the group to organize their manner into those are common to the group and those are applicable to individual companies, to ensure consistent manner within the group, and to be approved by the department in charge of group management.

III-4 Group-wide risk control framework

【Required actions for a financial institution: ii】

Establish programs for **information sharing within the group (Q1) (Q2)** required for **group-wide risk assessments (Q1)** and for ensuring the effectiveness of AML/CFT measures.

【Q1】

Regarding “group-wide risk assessments” or “information sharing within the group”, what kind of situation is assumed specifically?

【A】

“Group-wide risk assessment” is necessary to analyze and determine ML/FT risk of the acquired companies in advance, not only to the group that are currently forming, but also to newly formed group by, for example, acquiring domestic and overseas businesses.

In addition, "information sharing control framework within the group" refers to the information sharing control framework within the group that is required to ensure the effectiveness of AML/CFT. For example, while assuming that control framework includes the use and management of information shared within the group, while paying attention to laws and regulations related to information management in the host country.

【Q2】

To what extent can information be shared under Japanese legislation, such as Act on the Protection of Personal Information and the Financial Instruments and Exchange Act, in order to establish programs for information sharing for customer information and transaction information among domestic group companies?

【A】

(Relation to Act on the Protection of Personal Information)

Article 23, Paragraph 1 of Act on the Protection of Personal Information stipulates that in principle, the personal data must be provided to a third party with the consent of the individual. However, as an exception, in cases where “it is necessary for the protection of a person’s life, body or property and it is difficult to obtain the person’s content”, personal data may be provided to a third party without obtaining the person’s consent in advance.

Whether or not the case falls under the above exceptional cases is determined based on overall balance of interests in accordance with specific individual cases. According to 3-1-5 (2) of “the Guidelines on the Act on the Protection of Personal Information (General Rules)”, examples that may fall under this category include "information on anti-social

force such as organized crime group (Boryokudan), information on accounts used for remittance fraud, and information on persons who intentionally obstruct business". If the customer information or transaction information. In the event that customer information pertaining to suspicious transaction report based on APTCP corresponds to such information. However, it is necessary to determine whether or not the customer information or transaction information falls under the exception requirements referring to specific circumstances. Personal data that does not fall under the above exceptional case may be provided or shared based on the consent of the person (Article 23, Paragraph 5, Item 3 of the Act).

(Relation to the Financial Instruments and Exchange Act)

Under the Financial Instruments and Exchange Act, in principle, Financial Instruments Business Operators are restricted from receiving non-public information on customer within the group. However, this [Required actions for financial institutions] of the Guideline requiring "*Establish programs for information sharing within the group required for group-wide risk assessments and for ensuring the effectiveness of AML/CFT measures.*" is required for compliance with laws and regulations, and is considered to fall under the provision of exemptions from such restrictions (Article 153, Article 3, Item 1, etc. of Cabinet Office Ordinance Financial Instruments Business, etc.).

III-4 Group-wide risk control framework

【Required actions for a financial institution: iii】

Where a financial group operates through overseas offices, implement risk mitigation measures appropriate for the group as a whole, in compliance with each AML/CFT regulation applicable to its corresponding overseas operations and by allocating personnel in line with the risks, based on the identification and assessment of risks visualized through these processes and inherent to each overseas office.

【Q】

Regarding "where a financial group operates through overseas offices, implement risk mitigation measures appropriate for the group as a whole, in compliance with each AML/CFT regulation applicable to its corresponding overseas operations and by allocating personnel in line with the risks, based on the identification and assessment of risks visualized through these processes and inherent to each overseas office", what points are required to bear in mind specifically?

【A】

Financial institutions and other groups with overseas bases are required to identify and assess risks within the group in light of the laws and regulations related to AML/CFT applicable to overseas bases and to establish the location of risks at each overseas base, and then implement specific risk mitigation measures individually based on the results of these assessments.

Therefore, it is necessary for financial institutions and other groups with overseas bases to implement AML/CFT in order to be consistent with the laws and regulations applicable to each overseas bases. For example, when overseas offices receive an inspection and administrative order regarding ML/FT control framework from local supervisory authorities at overseas bases, the head office or the head office of the group groups need to receive reports in a timely and appropriate manner and take appropriate measures to respond to the issues pointed out or ordered.

III-4 Group-wide risk control framework

【Required actions for a financial institution: iv】

Where a financial group operates through overseas offices, in order to implement the AML/CFT measures consistently across the group in a timely and appropriate manner, **establish programs that enable sharing of necessary information and consolidated risk control framework (including the development and update of necessary IT systems), including the information about the customers and transactions involved in unusual transactions and the results of analyses as well as the status of STR**, **based on proper understanding of the information protection regulations** applicable to overseas offices and the stance of local regulators. (The necessity of such programs must be understood when formulating a business strategy for overseas operation.)

【Q】

Regarding "based on proper understanding of the information protection regulations" and "establish programs that enable sharing of necessary information and consolidated risk control framework (including the development and update of necessary IT systems), including the information about the customers and transactions involved in unusual transactions and the results of analyses as well as the status of STR", what points are required to bear in mind specifically?

【A】

Financial institutions and other groups with overseas bases are required to implement AML/CFT based on their understanding of the information protection regulations applicable to each overseas bases and the stance of foreign authorities. In particular, it is necessary to establish a control framework to properly classify information appropriate for group-wide control and information corresponding only to the country or region concerned, and to facilitate the sharing and integrated control of the required information, after understanding the operation of relevant authorities in the country or region concerned, such as information protection regulations in all countries and regions concerned.

III-4 Group-wide risk control framework

【Required actions for a financial institution: v】

Where a financial group operates through overseas offices, if the AML/CFT requirements of the jurisdiction in which each overseas office operates are less strict than those of Japan, apply and implement the group-wide policies, procedures and programs to those overseas offices in a consistent manner. If this is not permitted by the local regulation, inform the FSA. (Note)

(Note) If the requirements of a foreign jurisdiction are stricter than those of Japan, the local requirements must be followed.

【Q】

Regarding "where a financial group operates through overseas offices, if the AML/CFT requirements of the jurisdiction in which each overseas office operates are less strict than those of Japan, apply and implement the group-wide policies, procedures and programs to those overseas offices in a consistent manner. If this is not permitted by the local regulation, inform the FSA", what points are required to bear in mind specifically?

【A】

Financial institution group with overseas bases is required to promptly provide information to the Japanese authorities if the laws and regulations of the county / region which the overseas bases belong are not stricter than those of Japan and it is not permissible by the laws, and regulations of the county / region do not allow to implement AML/CFT measures required by Japan.

III-4 Group-wide risk control framework

【Required actions for a financial institution: vi】

In the case of Japanese offices of foreign financial groups, fulfill accountability to the authorities and other stakeholders for the ML/FT risk control framework of the group as a whole, and the status of transactions with Japanese institution, including correspondent banking relationships.

【Q】

Regarding "in the case of Japanese offices of foreign financial groups, fulfill accountability to the authorities and other stakeholders for the ML/FT risk control framework of the group as a whole, and the status of transactions with Japanese institution, including correspondent banking relationships", what points are required to bear in mind specifically?

【A】

In the event that Japan office of foreign financial group is required to explain the status of group-wide transactions with ML/FT risk control framework of the group as whole including correspondents, to its Japanese affiliates in Japan, it is required to fulfill its accountability to the authorities. Therefore, if it is unable to explain to the requests of the authorities, it is possibility that appropriate administrative measures will be taken.

III-5 Human resource development

（Main paragraph）

In order to ensure the effectiveness of ML/FT risk management, employees of branches and various other divisions must have the expertise and competency required for their roles, and properly implement policies, procedures, and programs prescribed by the Board.

Financial institutions are required to deepen their employee's understanding of AML/CFT measures, and maintain and improve expertise and competency for the entire organization, by hiring and training employees with such expertise and competency necessary for their roles through provision of appropriate **training (Q1)** (including the status of **relevant qualifications (Q2)** obtained) on an ongoing basis.

【Q1】

Does the term "training" include education through correspondence courses and e-learning?

【A】

"Training" may include such methods such as correspondence courses and e-learning.

【Q2】

What are "relevant qualifications" supposed to be? Are the qualifications not limited to those granted by external organizations, but also include in-house qualifications for in-house examinations?

【A】

Generally, "relevant qualifications" include qualifications granted by external organizations and industry associations, as well as internal qualifications that are encouraged to be obtained internally.

III-5 Human resource development

【Required actions for a financial institution: i】

Continually evaluate that **the employees involved in AML/CFT measures** have the knowledge and expertise required for such role, along with **the competency** to properly implement the measures including the identification and verification at the time of transactions and other measures after training.

【Q】

Does “the employees involved in AML/CFT measures” mean that they are responsible for internal control of such division? Or does it include employees in charge of business operation? In addition, what kind of method is assumed for the continuous confirmation of compliance?

【A】

"Employees involved in AML/CFT measures" refer to a wide range of employees involved in AML/CFT, including employees in charge of businesses operations. As described in the Guidelines, it is necessary to confirm whether the employee possesses the knowledge, expertise, conformity, etc. that are required according to the roles of the employee.

It is assumed that the method of confirmation will be confirmed through, for example, the status of training, the level of understanding of the training, and interviews by superiors, etc. However, specifically, it will be determined according to the content of the duties in charge and the characteristics of each financial institution.

III-5 Human resource development

【Required actions for a financial institution: ii】

In order to ensure that the employees have a proper understanding of specific CDD procedures including the identification and verification at the time of transactions according to their role, provide easy-to-understand material that helps them become familiar with the procedures, and other appropriate training on an ongoing basis.

【Q】

Regarding "in order to ensure that the employees have a proper understanding of specific CDD procedures including the identification and verification at the time of transactions according to their role, provide easy-to-understand material that helps them become familiar with the procedures, and other appropriate training on an ongoing basis", what points are required to bear in mind specifically?

【A】

In addition to providing knowledge on laws and regulation, training is also considered to provide necessary knowledge and insight according to the job responsibilities and work contents. Therefore, in order for employees to acquire necessary knowledge in accordance with their roles and to understand the situations in which they utilize the acquired knowledge in the flow of business operation, it is necessary to continuously implement training in accordance with the level of understanding of employees.

III-5 Human resource development

【Required actions for a financial institution: iii】

Analyze and examine whether the contents of such training are consistent with the risks being faced, whether they are in line with the latest laws and regulations, and information from domestic and foreign authorities and whether there is room for improvement from the perspective of dissemination.

【Q】

Regarding "analyze and examine whether the contents of such training are consistent with the risks being faced, whether they are in line with the latest laws and regulations, and information from domestic and foreign authorities and whether there is room for improvement from the perspective of dissemination", what kind of measures are required specifically?

【A】

As for training, it is important to conduct training and to improve the level of understanding of employees. However, it is equally important to appropriately review and consider improvements, etc. from the viewpoint of whether the content of the training itself is based on the views of domestic and foreign authorities, and whether it is sufficient for employees.

It is also important to take into account the size and characteristics of financial institutions. For example, where a financial group operates through overseas offices, in addition to creating and distributing materials on risk assessment methodologies for the employees in charge of conducting risk assessment in each overseas office, it is possible to provide training about the importance of risk assessment and the correct way of assessing risks, taking into account the unique and specific situation of each office, and review the contents of the training on an ongoing basis. In addition, where a financial group operates through overseas offices and the overseas operations are strategically important for the institution, it is possible to establish programs for the employees in charge of AML/CFT measures to undergo effective training and obtain relevant qualifications in relation to international trends concerning ML/FT.

III-5 Human resource development

【Required actions for a financial institution: iv】
Evaluate the effectiveness of training, by examining whether the procedures outlined in the training content are being following up with the employee (Q1). **Review the number of participants, frequency, status, and content of training, etc. as necessary (Q2)**, taking into account any emerging risks.

【Q1】

Regarding "evaluate the effectiveness of training, by examining whether the procedures outlined in the training content are being following up with the employee", what kind of measures are required specifically?

【A】

The purpose of the training to implement effective AML/CFT measures. Therefore, the content of the training should be practical in order to reduce the risks faced by financial institutions. In this case, it is necessary for employees who have received training to utilize the acquired knowledge and appropriately fulfill the roles required in the course of business. Therefore, it is necessary to conduct follow-up to ensure that knowledge is firmly established and to confirm whether there is any expected business effect, taking into account the work of employees and to examine whether there is room for improvement.

【Q2】

Regarding "review the number of participants, frequency, status, and content of training, etc. as necessary", what kind of measures are required specifically?

【A】

If the contents of the NRA, the FATF's recommendations, explanatory notes, sector-specific guidance etc., are revised, or if there is a change in the risks faced by financial institutions, it will be necessary to update the existing training as necessary, and to conduct a verification for those who have already taken the training.

III-5 Human resource development

【Required actions for a financial institution: v】

Deepen the risk awareness of the business division, for example, by sharing the information about the firm-wide STR status and providing responses to questions, and by ensuring the information be available to each employee within the business division.

【Q】

Regarding "deepen the risk awareness of the business division, for example, by sharing the information about the firm-wide STR status and providing responses to questions, and by ensuring the information be available to each employee within the business division", what kind of measures are required specifically?

【A】

In terms of effective AML/CFT measures, it is important to make business division, which directly confront customers, fully aware of the ML/FT risks faced by financial institution. In this case, it is necessary for the management division which collect various information, to make the business division aware of the ML/FT risks faced by financial institution while disclosing information and best practices regarding risks faced by financial institution and best practices based on the results of the analysis of STR.

It is also important for the business division to utilize the risk information provided by its own operations.

End