

[Provisional Translation]

The original texts of the Guidelines 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 Guidelines and is subject to any future changes.

Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism

April 10, 2019

Financial Services Agency

| | | |
|--------------|--|-----------|
| I | General Concepts..... | 1 |
| I-1 | Risk-based approach..... | 1 |
| I-2 | Financial institutions' AML/CFT measures | 3 |
| (1) | ML/FT risk management..... | 3 |
| (2) | Involvement and understanding of management..... | 4 |
| I-3 | Roles of industry associations and central institutions | 4 |
| I-4 | Supervisory actions | 5 |
| II | Risk-Based Approach..... | 6 |
| II-1 | Risk-based approach..... | 6 |
| II-2 | Identification, assessment, and mitigation of risk..... | 6 |
| (1) | Risk identification..... | 7 |
| (2) | Risk assessment..... | 8 |
| (3) | Risk mitigation..... | 9 |
| (i) | Risk mitigation measures | 9 |
| (ii) | Customer due diligence (CDD)..... | 10 |
| (iii) | Transaction monitoring and screening | 14 |
| (iv) | Record keeping..... | 15 |
| (v) | Suspicious transaction reporting (STR)..... | 15 |
| (vi) | IT systems | 16 |
| (vii) | Data governance..... | 17 |
| (4) | Foreign remittance..... | 18 |
| (5) | FinTech..... | 20 |
| III | Evaluation and Review of the ML/FT Risk Management and Its Effectiveness..... | 20 |
| III-1 | Formulation, implementation, evaluation, and review of AML/CFT policies, procedures and programs (PDCA) | 21 |
| III-2 | Involvement and understanding of management | 22 |
| III-3 | Management and control: three lines of defense | 23 |
| III-4 | Group-wide risk management..... | 26 |
| III-5 | Human resource development..... | 28 |
| IV | Monitoring and Public Private Partnership..... | 29 |
| IV-1 | Monitoring by the Financial Services Agency..... | 29 |
| IV-2 | Public private partnership and cooperation with relevant authorities | 30 |

I General Concepts

I-1 Risk-based approach

The basic requirements on anti-money laundering and combating the financing of terrorism (“AML/CFT”) in Japan, such as identification and verification at the time of transactions, are prescribed in the Act on Prevention of Transfer of Criminal Proceeds (“Criminal Proceeds Act”), the Foreign Exchange and Foreign Trade Act (“Foreign Exchange Act”), and other relevant laws and regulations.

Financial institutions licensed or registered to conduct operations under the Banking Act, the Insurance Business Act, the Financial Instruments and Exchange Act, and other laws that introduce legislation for each type of business in the financial industry are legally regarded as a “specified business operator” under the Criminal Proceeds Act, as well as “Banks, etc.” or “Financial institutions, etc.” under the Foreign Exchange Act, and therefore are subject to relevant requirements prescribed in such laws and regulations.

Since a financial system is a network of various flows of funds in the diversified forms of remittances, settlements, and money transfers conducted by the financial institutions, in order to ensure the soundness of the entire financial system, it is vital that individual financial institutions participating in the financial system shall build and maintain solid risk management commensurate with their operations and roles in the financial system.

AML/CFT measures that a financial institution should take are substantially influenced by ever-changing international affairs, as well as the constantly evolving actions by other financial institutions against such external circumstances. Financial institutions need to swiftly respond to the changes in such circumstances and their corresponding risk profiles, and effectively maintain their money laundering and the financing of terrorism (“ML/FT”) risk management.

Implementing such swift and effective countermeasures requires financial institutions to appropriately identify and assess the ML/FT risks they face in a timely manner – including risks relating to their customers’ operations –, and to undertake mitigation measures commensurate with those risks, namely a *risk-based approach*.

The risk-based approach for ML/FT risk management is established as a central principle of the Financial Action Task Force (“FATF”) Recommendations, and has equally been an established practice in major developed countries. With the need for swift and effective measures, the risk-based approach is a minimum standard that financial institutions participating in Japan’s financial system should implement.

In particular, under the increasing threat of terrorism faced by the international community,

close attention is necessary for the fact that calls for stricter AML/CFT measures have rapidly increased, as seen in the past cases in which inadequate AML/CFT measures led financial institutions to face large fines from foreign authorities or the termination of correspondent banking arrangements from their foreign counterparties.

Taking proper actions by Japan's financial system in response to such calls is necessary. In particular, those financial institutions engaging in foreign remittances need to sufficiently respond to supervision by foreign authorities and other international AML/CFT developments.

As the threat of terrorism has spread across borders, financial institutions shall establish effective risk management for terrorist financing with the awareness that their products and services can be abused as tools for terrorist financing. For example, in the case where a financial institution conducts a transaction with a non-profit organization, it is important for financial institutions to be aware that they are at risk of being exploited for terrorist financing depending on the nature and areas of their activities, while presuming that not all non-profit organizations are inherently higher-risk customers, and to take necessary risk mitigation measures taking into account the National Risk Assessment (Japanese NRA as provided for in the Criminal Proceeds Act) and the analyses by the FATF.

Financial institutions shall establish appropriate risk management, including measures addressing the financing of proliferation of weapons of mass destruction, taking into account relevant foreign and domestic laws and regulations such as the Foreign Exchange Act and the Act on Special Measures Concerning International Terrorist Assets Freezing.

To this end, financial institutions need to continuously improve AML/CFT measures through a firm-wide governance structure involving different divisions and geographic areas and facilitating the proactive involvement of management, thereby ensuring that AML/CFT measures effectively function in business divisions that principally serve customers.

Financial institutions should develop in their business strategies forward-looking actions for strengthening their AML/CFT measures for preventing the future misuse of their functions. They should also fulfill their accountability to a wide range of stakeholders including customers and authorities with regard to their policies, procedures, programs as well as their implementation status by disclosing relevant data.

The Financial Services Agency ("FSA"), with necessary supervisory measures, shall monitor the AML/CFT measures of each financial institution, share the outcome with financial institutions, and urge them to enhance risk management.

The Guidelines clarify the *required actions* and *expected actions* to be implemented by each financial institution and how the FSA shall conduct monitoring going forward.

Furthermore, in an effort to encourage financial institutions to make forward-looking enhancements, the Guidelines provide better examples found through the past monitoring or in foreign financial institutions as *cases of advanced practices*, as a reference for financial institutions to pursue best practices.

The Guidelines also explain the roles of industry associations and central institutions and coordination with the authorities, with a view in particular to helping financial institutions with small sizes or limited scope of transactions to develop effective risk management programs.

I-2 Financial institutions' AML/CFT measures

(1) ML/FT risk management

Financial institutions are required to identify and assess their ML/FT risks based on an overall group-wide understanding of their products and services, transaction types, countries and geographic areas, and customer attributes, and to implement mitigation measures commensurate with such risks, taking into account their business environment and strategies as well as their risk tolerances.

In order to swiftly undertake measures commensurate with those risks that reflect ever-changing international circumstances and the evolving responses by other financial institutions, it is vital not only to address individual cases or problems, but rather, with the involvement and understanding of management, to undertake holistic forward-looking evaluation including the necessity for reforming their management and risk management programs, and develop a group-wide effective ML/FT risk management.

To address this perspective, the FSA plans to regularly review the Guidelines. Equally, financial institutions are required to establish and maintain their risk management reflecting the substantive contents of related laws and regulations and the Guidelines, not focusing exclusively on compliance with those regulations and the Guidelines and checking technical compliance with them.

While there are differences between the risks of money laundering and the financing of terrorism – such as the purpose, size, and value of those transactions as well as the countries or geographic areas that need caution upon executing those transactions – the basic frameworks required to maintain the soundness of the financial system do not differ fundamentally among those transactions. The Guidelines therefore explain AML and CFT simultaneously.

(2) Involvement and understanding of management

When developing the aforementioned ML/FT risk management, the proactive involvement of management, based on the understanding that ML/FT risk can be significant for the entire firm, is indispensable. In fact, AML/CFT measures shall not solely be left to the related divisions.

The proactive engagement and leadership of management would be necessary, for example, in conducting a forward-looking gap analysis, taking cross-organizational measures involving multiple divisions, and strategically hiring and training their personnel and allocating resources according to their expertise and experience. In order to disseminate AML/CFT initiatives to all executives and employees, it would also be important to demonstrate management's proactive commitment toward AML/CFT and convey their messages, such as by taking into account AML/CFT in the performance evaluation of employees.

It is vital for management to increase the awareness of AML/CFT based on an appropriate understanding of ML/FT risks, and promote more advanced cross-organizational measures by their top-down initiatives. After all, the responsibility for fulfilling accountability outlined in I-1 above for strengthening the ML/FT risk management is to be primarily assumed by management.

I-3 Roles of industry associations and central institutions

Information gathering by an individual financial institution with respect to advanced practices on a risk-based approach or international developments in AML/CFT may sometimes qualitatively and quantitatively be limited. As the methods of ML/FT are constantly changing, it may be especially difficult for financial institutions with small sizes or limited scope of transactions to accumulate sufficient information or expertise by themselves.

In order to lift the level of the entire Japanese financial system, it is essential for industry associations, central institutions, etc., to take central and guiding roles in improving their member financial institutions' ML/FT risk management, in coordination with the authorities. This includes sharing of information and cases to which financial institutions should refer, providing support for risk management development, promoting industry-wide joint operations via appropriate shared IT systems, and encouraging broader user understanding.

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 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 management to undertake AML/CFT in accordance with the risk-based approach.

I-4 Supervisory actions

Keeping Japan's financial system sound and immune from ML/FT is extremely important, and as the financial authority, the FSA properly conducts the 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 the inadequate implementation of *required actions* in the Guidelines, 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.

In addition to the *required actions* that financial institutions are required to implement, the AML/CFT Guidelines provide *expected actions* as further measures that financial institutions of a certain size and operation or in specific circumstances are encouraged to take to enhance their risk management and programs.

The amended Criminal Proceeds Act, which came into effect in October 2016, introduced risk assessment by the government and *specified business operators*. The Guidelines provide the *required actions* and *expected actions*, encompassing those requirements under the amended Criminal Proceeds Act and other necessary or expected measures, with the purpose of ensuring financial institutions' effective risk identification, assessment, and mitigation with a risk-based approach. Even if not described in the Guidelines, financial institutions are subject to the Supervisory Guidelines for each business category and to other regulatory documents relating to all specified business operators, in particular, *Points to Note regarding the Criminal Proceeds Act* and *List of Reference Cases of Suspicious Transactions*, published by the FSA.

Effective AML/CFT measures such as a risk-based approach are an international requirement of financial institutions, and therefore they should pay adequate attention to the documents issued by the FATF, the Basel Committee on Banking Supervision, and other international bodies.

The Guidelines apply to firms that fall under the category of the specified business operators as prescribed in Article 2, paragraph 2 of the Criminal Proceeds Act and are under the supervision of the FSA with the exception of the entities listed in item 46 of the

said paragraph (“[a] financial institution[s]”).

II Risk-Based Approach

II-1 Risk-based approach

A risk-based approach in AML/CFT refers to an approach that financial institutions identify and assess their ML/FT risks and implement effective mitigation measures commensurate with those identified risks.

The types and techniques of ML/FT are constantly changing in conjunction with crime and other underlying trends, as well as broader socioeconomic conditions such as industry and employment conditions, demographic movements, legal systems, new forms of transaction types due to advances in information technology (“IT”), and the globalization of the economy and financial services.

With the changes in the ML/FT methods, AML/CFT measures should be constantly enhanced. The increased convenience and speed of information transfer in recent years has exacerbated the risk that financial institutions that have fallen behind in implementing the enhancements will be targeted for the purpose of ML/FT.

Financial institutions need to take effective actions through the risk-based approach, in order to appropriately identify and assess ML/FT risks by themselves and prioritize and swiftly improve ML/FT risk management commensurate with the risks.

The risk-based approach has become an international standard, as set out in the Financial Action Task Force (“FATF”) Recommendation 1 as an underlying principle in the whole document. ^(Note)

(Note) The FATF Recommendations state that “countries should identify, assess, and understand the money laundering and terrorist financing risks for the country” and financial institutions “should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks” for products and services they handle, requiring both countries and financial institutions to respectively implement risk-based approaches.

II-2 Identification, assessment, and mitigation of risk

It is important under the risk-based approach to consider necessary actions against ML/FT risks step-by-step, for instance by categorizing them in stages of risk identification, assessment, and mitigation.

(1) Risk identification

Risk identification is a process to identify ML/FT risks faced by a financial institution through comprehensive and specific risk evaluation of the products and services offered, transaction types, the countries and geographic areas of transactions, customer attributes, and other relevant factors, and is the starting point of a risk-based approach.

When conducting the comprehensive and specific evaluation, the collection of internal information needs to be aggregated and analyzed from a firm-wide perspective. Therefore, this task should not be delegated solely to the division in charge of AML/CFT; rather, it should be performed under the coordination and cooperation of all relevant divisions with the proactive involvement of management.

When undertaking 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, which captures each characteristic.

Further, such analyses tend to focus on general matters that are common to multiple financial institutions. Financial institutions therefore need not only to refer to these analyses, but also to comprehensively and specifically capture the characteristics of their businesses and identify the risks they by themselves face.

Required actions for a financial institution

A financial institution shall:

- i. Identify the ML/FT risks it faces by comprehensively and specifically evaluating risks 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.
- ii. When conducting a comprehensive and specific evaluation, consider the results of the national risk assessment, at the same time taking into account the financial institution's specific features such as the geographic attributes of its business region, business environment, and management strategy, etc.
- 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.
- iv. When handling new products and services, or conducting transactions using new technologies or those with new characteristics, analyze and evaluate their ML/FT risks before offering such products and services.
- v. Conduct comprehensive and specific evaluation of ML/FT risks with the coordination

and cooperation of all relevant divisions, under the proactive involvement of management.

Expected actions for a financial institution

- A. 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, for example, the number and amount of foreign remittance transactions, non-face-to-face transactions, and non-resident transactions, 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.
- B. When it files a certain amount of suspicious transaction reports, analyze comparable and quantitative information, such as the number of reports and transaction volumes among divisions and sections, and improve the effectiveness of the financial institution's risk evaluation.

(2) Risk assessment

Risk assessment is a process to assess the level of impact on a financial institution of the ML/FT risks identified in the preceding (1), and formulates the basis for specific actions such as mitigation measures. The risk assessment therefore needs to reflect the characteristics of the financial institution's business environment and the business strategy.

As the risk assessment is directly linked to the specific details of risk mitigation measures and the (re)allocation of resources, it needs to be conducted in a firm-wide and consistent manner with the involvement of management.

Required actions for a financial institution

A financial institution shall:

- i. Implement the same actions in risk assessment as the *required actions* in “(1) Risk identification” above.
- ii. Establish firm-wide policies and specific approaches for risk assessment, and in line with such policies and approaches conduct the assessment based on the specific and objective grounds.
- iii. Document the results of the risk assessment, and utilize them for developing measures necessary for risk mitigation.
- iv. Conduct the review of the risk assessment regularly at least once a year, as well as when an event such as the occurrence of new risks and the introduction of new regulation that may have a significant impact on AML/CFT measures occurs.
- v. Involve management in the processes of risk assessment, and obtain approval from management for the results of the risk assessment.

Expected actions for a financial institution

- A. Implement the same actions in risk assessment as the *expected actions* in “(1) Risk identification” above.
- B. When products and services it offers, transaction types, countries and geographic areas of transactions, customer attributes, etc., are wide-ranging, break down the associated risks into smaller categories, assess risks for each category, and reassess them by combining results of each category, so that the result of the firm-wide risk assessment is visualized in a risk map and reviewed in a timely manner.

Cases of advanced practices :

a case where a financial institution’s risk management division conducts risk assessment consistently for the entire firm encompassing both front-office and back-office divisions, by combining the results of risk assessment based on detailed quantitative data with qualitative information such as feed-back from front-office divisions.

Specifically, the control division collects quantitative data about suspicious transaction reports, including not only the total number of reports, but also more detailed indicators such as breakdown by branch, reason for reporting, and detection scenario. Then it conducts a primary risk assessment that reflects scores and changes of those risk indicators by product and service, transaction type, country or geographic areas, customer attribute and others.

Further, based on the primary risk assessment using such quantitative data, the control division sends a questionnaire to the front-line and other divisions to collect qualitative risk information such as transaction type and customer type, which are relevant to their daily business operations, and finalizes its risk assessment by adjusting the aforementioned primary risk assessment with such qualitative information.

(3) Risk mitigation

(i) Risk mitigation measures

Risk mitigation is a process to conduct measures to mitigate a financial institution’s ML/FT risks and dictates the effectiveness of the institution’s ML/FT risk management.

Under a risk-based approach, financial institutions are required to collect and verify information about specific customers’ profiles and activities, compare that information with the results of risk assessment conducted in accordance with aforementioned (1) and (2), and determine and implement effective measures to mitigate those identified risks.

(Note)

(Note) In the Guidelines, “customer due diligence” (“CDD”) refers to, among other mitigation measures, a series of processes in which a financial institution collects and verifies actual information about specific customers and their activities and transactions in light of the results of its own risk assessment, compares that information with the results of the risk assessment, and determines and implements effective measures necessary to mitigate those identified risks. Apart from the approach that focuses on each customer, there are other approaches that focus on each transaction to analyze and detect unusual transactions. It is effective to combine both approaches for risk mitigation.

Risk mitigation measures must be implemented according to the level of the risks posed by each individual customer and their transactions. Enhanced measures are required when a financial institution finds high risks based on its own criteria, whereas simplified measures are allowed when the financial institution finds lower risks.

Each financial institution should, in accordance with risks it faces, consider and implement the contents of risk mitigation measures individually and specifically for each customer and transaction. In addition to the items listed in the Guidelines, financial institutions are required to devise mitigation measures commensurate with their risks while also referring to information provided by relevant domestic and foreign authorities and case examples shared through their industry associations.

Required actions for a financial institution

A financial institution shall:

- i. Collect and verify actual information about customers and their activities and transactions, compare that information with the results of risk assessment, and determine and implement effective measures to mitigate those identified risks.
- 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 programs developed by the 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.

(ii) Customer due diligence (CDD)

As noted above, “customer due diligence” (“CDD”) in the Guidelines is, among other mitigation measures, a series of processes in which a financial institution identifies and assesses ML/FT risks with regard to a specific customer, reviews the information about the customer and their transactions in light of the results of risk assessment, and determines the measures necessary to mitigate the identified risks, and is the core element

of risk mitigation measures.

When a financial institution transacts with a customer, it is vital that it collects and verifies fundamental information about the customer, such as who the individuals or entities including legal arrangements or its beneficial owners are, what they do, why they would like to conduct transactions, and where their funds come from. It then needs to consider and implement appropriate mitigation measures based on such information collected and verified.

The processes of CDD may be expediently categorized into three stages; the start, continuation, and end of the business relationship. Each financial institution should determine and implement appropriate mitigation measures at each of the stages according to the level of risks posed by the individual customers and their transactions.

Financial institutions must conduct risk assessment for all of their customers, based on a comprehensive consideration of the all information obtained through the processes above. Enhanced due diligence (“EDD”) is required for customers who are considered to have high ML/FT risks, including but not limited to foreign politically exposed persons (“PEPs”) ^(Note 1) or those conducting transactions associated with Specified Jurisdictions ^(Note 2). In contrast, if risks are determined to be low, conducting simplified due diligence (“SDD”) and ensuring the smooth execution of transactions is important.

(Note 1) Foreign PEPs as defined in each item of paragraph 3, Article 12 of the Order for Enforcement of the Criminal Proceeds Act and Article 15 of the Ordinance for Enforcement of the Criminal Proceeds Act.

(Note 2) Jurisdictions as specified in each item of paragraph 2, Article 12 of the Order for Enforcement of the Criminal Proceeds Act.

Required actions for a financial institution

A financial institution shall:

- i. Formulate a customer acceptance policy, 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.
- ii. When formulating the customer acceptance policies in i. above, consider customers’ and beneficial owners’ occupations and business activities and other various information 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.
- iii. Seek reliable evidence when surveying information relevant to a customer and its beneficial owner and the purpose of transaction, including identity information 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.

- iv. Comply with, and take other necessary measures against, applicable economic and trade sanction laws and regulations enforced by Japanese and other foreign authorities, such as by screening the names of a customer and beneficial owners against the sanction lists published by each regulator.
- v. Establish a framework to properly detect high-risk customers in accordance with the size and characteristics of the financial institution, by utilizing reliable databases and systems or other rational measures.
- vi. Conduct customer risk assessment for all the customers by, for example, assessing risks of respective customer types grouped by common characteristics (such as products/services or customer attributes) shared by customers, while combining the ML/FT risk assessment results for each factor such as products and services, transaction types, countries and geographic areas, and customer attributes, etc., and, determine mitigation measures in accordance with the customer risk assessment.
- vii. For customers determined to have high ML/FT risk, apply enhanced due diligence (EDD) measures including the following:
 - a. Obtain additional information in accordance with the risk, especially that on customer's state of assets and incomes, purpose of transactions, occupation, title, and source of funds;
 - b. Obtain the approval of senior management 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, in accordance with the risk; and
 - d. Examine the need for raising the risk level for other customers with similar attributes to such customers.
- viii. For customers determined to have low ML/FT risk, give due consideration for smooth execution of transactions by implementing simplified due diligence (SDD) measures taking into account the nature of the risk, such as relaxing the transaction monitoring thresholds for transactions conducted by such customers.^{(Note 1) (Note 2)}

(Note 1) Even in this case, financial institutions must comply with the laws and regulations of Japan and other jurisdictions applicable to such transactions.

(Note 2) FATF and BCBS cite routine and small transactions by individuals as examples of transactions that do not require EDD.
- ix. 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 such as identity information, the purpose of transactions, the occupation, business details, the state of assets of the customer and beneficial owner, and incomes and sources of their funds, taking into account the results of the institution's risk assessment and transaction monitoring with respect to transaction types and customer types 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;
 - c. Appropriately manage the records of investigations, including the communication with the customer, and share these with the relevant executives and employees;
 - d. Review and update customers' information when an event occurs that may increase the customer's risk, as well as on a periodic basis with different frequency according to the customer's risk, such as more frequency reviews for higher-risk customers and less frequent reviews for lower-risk customers; and
 - e. Review the customer risk assessment based on customers' information obtained in the process of ongoing CDD.
- x. For customers and transactions with which CDD measures a financial institution determines to be adequate cannot be completed, including cases where the customer refuses to provide requested CDD information, consider appropriate measures to eliminate the risk, 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 and that AML/CFT requirements are not used as an excuse for rejecting the customer.

Expected actions for a financial institution

- A. Introduce an indicator that objectively measures the risk level of each customer (i.e., customer risk rating), which combines the assessment results for each category such as products and services, transaction types, countries and geographic areas, customer attributes, etc., and review the rating.
- B. Conduct measures such as a face-to-face meeting with a customer and/or beneficial owner and an on-site visit for those whose business office has not been yet confirmed, before entering into the transaction or executing large transactions with customers whose businesses or locations are obscure.

Cases of advanced practices :

a case related to ongoing CDD measures where a financial institution quantitatively and systematically recognizes each customer's risk and assigns a risk rating to the customer based on its own risk assessment and takes enhanced measures for high-risk customers such as increasing the frequency of regular reviews.

Specifically, customer risk rating is assigned by a model which quantifies and aggregates the risks for products and services, transaction types, countries and geographic areas, customer attributes, etc. The risk model is incorporated into the institution's systems so that the risk rating is updated in a timely and flexible manner, at the time of the customer onboarding and whenever there is a change in the customer's CDD information.

Furthermore, efforts are made to mitigate risks of high-risk customers according to the

actual situation, for example, by lowering thresholds of the transaction monitoring system for detecting unusual transactions or by increasing the frequency for negative information searches using external data. In addition, the institution confirms whenever there is any discrepancy between the initial purpose of the relationship and the actual activities of the customer by updating the information with a questionnaire or on-site visits.

Cases of advanced practices :

a case related to the effectiveness of CDD based on customer risk ratings.

Specifically, a specialist team within control divisions that has expertise in both IT and AML/CFT measures periodically validates the customer risk rating models and systems from the viewpoints whether the results are consistent with the results of the institution's risk assessment, whether the risk ratings given by the models/systems correctly reflect the individual customers' risks, and whether the mitigating measures for a specific risk rating are appropriate for the risks identified.

Cases of advanced practices :

a case where a financial institution conducts ongoing CDD of foreign PEPs in a more refined and specific manner.

Specifically, the institution gathers information such as whether a customer is a foreign PEP or not, his or her position and function, the length of time since he or she has quitted their positions, and his or her purpose of transactions. Based on the information and their country of residence, etc., the institution assigns a foreign PEP risk rating, subdividing its general customer risk ratings. Then the institution adjusts the scope and frequency of CDD of each customer according to the risk ratings.

(iii) Transaction monitoring and screening

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.

Required actions for a financial institution

- i. A financial institution shall conduct appropriate transaction monitoring and screening for individual transactions to detect unusual transactions and transactions subject to sanctions, taking into account the results of risk assessment of specific types of transactions.

(iv) Record keeping

The customer identification records and transaction records maintained by financial institutions not only provide the status and results of their CDD, but also represent essential information for submitting required data to the authorities and for determining the necessity for filing a suspicious transaction report.

Required actions for a financial institution

- i. A financial institution shall maintain 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.

(v) Suspicious transaction reporting (STR)

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

In addition, suspicious transaction reports can be utilized to strengthen their ML/FT risk management by analyzing them together with other indicators.

Required actions for a financial institution

A financial institution shall:

- 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.
- ii. Establish programs for monitoring, detecting and analyzing suspicious customers and transactions, utilizing IT systems/manuals fit for the business operations of the financial institution.
- iii. In determining whether STR is necessary or not, consider the results of the national risk assessment; customer attributes such as involvement of a foreign PEP and the customer's business activity; the countries and geographic areas involved in transactions; the form of transactions including the amount and frequency in light of the customer's profile; and other circumstances.
- iv. In determining whether STR is necessary or not, review a transaction's nature such as whether it is an ongoing transaction with an existing customer or a one-off transaction with a walk-in customer.
- v. Promptly file a report once a transaction is determined to be suspicious.
- 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.

- vii. For customers who are determined to have high risk due to their suspicious transactions, such as being the subject of multiple STRs, conduct appropriate mitigation measures commensurate with their risks.

(vi) IT systems

Utilizing IT systems including software enables the integrated management of various information associated with the transactions of financial institutions with their customers, such as products and services, transaction types, countries and geographic areas, and customer attributes.

In addition, the proper utilization of IT systems enables automated detection of unusual transactions, trend analysis of customers and transactions, and risk rating of customers. It also facilitates a financial institution to add or change scenarios for detection of suspicious activities or to flexibly adjust thresholds, thereby strengthening its ML/FT risk management.

In order to properly utilize an IT system for AML/CFT, it is important to establish well-designed IT systems, evaluate their effectiveness, and update them on a timely basis. These require evaluating the system from operational aspects, such as whether the scenarios and thresholds are adequate in light of risks being faced and whether the sanction lists used for screening of the recipients of remittances and goods imported/exported are up-to-date.

Required actions for a financial institution

A financial institution shall:

- 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 vii. below for the system.
- ii. Proactively utilize the IT system to increase the effectiveness of transaction monitoring and other AML/CFT measures, for example, by setting up detection standards such as a scenario or threshold that reflect the results of risk assessment.
- iii. Periodically and at any time whenever a problem happens evaluate whether the design and operation of the AML/CFT systems are appropriate in light of the results of risk assessment; and improve both the design and operation of the systems based on the evaluation results.
- iv. Review and improve the detection standards such as a scenario or threshold, through ongoing analysis of indicators such as the number of system-detected cases and suspicious transaction reports by transaction type (e.g., industry, geographic area) and detection standard (e.g., scenario, threshold), as well as non-system related

information.

- v. Ensure that the transaction screening system is properly operating, for example, by verifying whether the sanction lists used for screening of the recipients of remittances and goods imported/exported are up-to-date.
- vi. Evaluate the effectiveness of the IT system by reviewing, for example, the scenarios and thresholds of transaction monitoring systems, and examination processes for detected cases by business and control divisions through an independent evaluation process such as internal and external audits.
- vii. Even if a financial institution outsources system operations to a contractor shared with other financial institutions or uses a joint system, analyze the characteristics of its own transactions and associated risks, evaluate the adequacy of the outsourced operations in light of the results of such analysis, and take additional measures.

Cases of advanced practices :

a case where a financial institution increases the flexibility and effectiveness of mitigation measures by taking advantage of IT systems that enable quick revisions and updates of risk assessment results and risk ratings.

Specifically, the financial institution allocates personnel that have expertise in data analytics to the division responsible for AML/CFT risk assessment and risk rating, to establish programs that enable quick revisions and updates of risk assessment and risk rating results, by reflecting real-time data about the individual customers and transactions.

These revisions and updates allow the financial institution to promptly adjust mitigation measures according to the level of ML/FT risks, for example, by adjusting the scope and thresholds of unusual transactions to be detected, or by setting a system-flag of prohibited transfers for certain transactions.

(vii) Data governance

The effectiveness of IT systems can only be ensured with the accuracy of data such as customer information, customer identification records, and transaction records, each of which is used in those IT systems.

In addition to ensuring the accuracy of customer identification records and transactions records, financial institutions are required to appropriately manage data as a prerequisite for effective use of IT systems, by collecting and storing accurate data and organizing it into analyzable ways.

Required actions for a financial institution

A financial institution shall:

- 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, by collecting and storing accurate data and organizing it in a manner capable of analysis.
- ii. Periodically validate integrity and accuracy of the data used for IT systems such as customer information, customer identification records, and transaction records.
- 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. 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 possessing qualifications); and
 - c. Reports to managements on ML/FT risk management, and the records of their discussions.

(4) Foreign remittance

When a financial institution handles foreign remittance by itself or through other financial institutions, it is required to undertake necessary measures such as screening of the transaction against the applicable sanction lists of relevant jurisdictions, in accordance with the Foreign Exchange Act and other domestic and foreign laws and regulations regarding foreign remittance.

It should be emphasized that cross-border banking services, such as foreign remittance, involve different ML/FT risks to domestic banking services that complete locally, in that it is more difficult for the financial institution to monitor the parties involved in foreign transactions. Financial institutions therefore need to consider such differences in risks as well as the trends of foreign regulations and international discussions, in order to adequately identify, assess, and mitigate risks.

When financial institutions have correspondent banking arrangements with other financial institutions or handle foreign remittance transactions on behalf of other financial institutions, the effectiveness of measures for mitigating ML/FT risks is dependent on effectiveness of ML/FT risk management of their counterparties to the arrangement. Hence, the financial institution is required to appropriately monitor the effectiveness of ML/FT risk management of its counterparties.

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.

Furthermore, even when a financial institution outsources foreign remittances to other financial institutions, the outsourcing institution is required to identify, assess, and mitigate the ML/FT risks associated with foreign remittances as is the case for other business that they conduct by themselves.

Required actions for a financial institution

A financial institution shall:

- 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.
- ii. Ensure that the ordering or intermediary financial institution informs the intermediary or beneficiary financial institution of the remitter and recipient information in accordance with international standards, so that the intermediary or beneficiary institution is aware of the risks involved in the foreign remittance. Where the information is missing, the intermediary or beneficiary institution is required to take adequate measures commensurate with the risk.
- 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 the Criminal Proceeds Act and Articles 28 and 32 of the Ordinance for Enforcement of the Act. In addition, establish programs for confirming the ML/FT risk management of the respondent institution and conduct periodic reviews.
- iv. 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.
- v. When undertaking foreign remittances for other financial institutions, monitor the ML/FT risk management of the counterparty institution by questionnaire, on-site visit and/or other measures, including their customer identification/due diligence programs relating to foreign remittances.
- vi. When outsourcing foreign remittances to other financial institutions, evaluate the nature of the foreign remittances under the financial institution's risk-based approach, and steadily identify, assess and mitigate the associated ML/FT risks.

Expected actions for a financial institution

- A. Assign a risk rating to respondent institutions that pose varying level of risks, in light of the respondent's jurisdiction, customer base, business, ML/FT risk management, AML/CFT regulations and supervision of the respondent's jurisdiction and other factors, and change the frequency of reviews according to the level of risks.

Cases of advanced practices :

a case where a financial institution improves the effectiveness of the risk management on correspondent banking relationships by gathering detailed information through on-site visits (including the interviews of the respondents about their AML controls and visits to local regulators) together with document reviews, and assigns detailed risk ratings based on the results of such due diligence.

(5) FinTech

New technologies such as AI (artificial intelligence), block chain, and RPA ^(Note) are used in various phases of AML/CFT to improve the effectiveness of controls, including the identification and verification at the time of transactions and the detection and reporting of suspicious transactions.

These new technologies are expected to be utilized to a greater extent in AML/CFT measures. Financial institutions are expected to examine the benefits of new technologies and proactively explore the possibility for leveraging them for sophistication and streamlining of AML/CFT controls, taking into account the practices of other financial institutions and issues surrounding the introduction of new technologies.

(Note) Robotic process automation: Using artificial intelligence to automate routine jobs such as document preparation and data input.

Expected actions for a financial institution

- A. Examine the benefits of new technologies and proactively explore the possibilities for leveraging them for sophistication and streamlining of AML/CFT controls, taking into account the practices of other institutions and issues surrounding the introduction of new technologies.

III Evaluation and Review of the ML/FT Risk Management and Its Effectiveness

In order to ensure the effectiveness of AML/CFT measures, financial institutions are required to establish an effective ML/FT risk management by formulating their policies, procedures, and programs, and implement them consistently throughout the organization with the involvement of management.

Financial institutions are required to regularly evaluate the effectiveness of their AML/CFT that are based on those policies, procedures and programs, and to make constant efforts to improve effectiveness of the AML/CFT based on such evaluation and through necessary revisions.

In order to establish such firm-wide risk management, a robust governance structure must be built, with the understanding and active involvement of management, including the appointment of an executive with the responsibility and authority to implement AML/CFT measures, and clear definition of the roles and responsibilities of each division.

In addition, a financial institution that forms a financial group or operates globally is required to formulate AML/CFT policies, procedures, and programs, and apply them consistently across the groups and globally, taking into account the differences in the business categories of group entities, and the countries and geographic areas in which they operate.

Furthermore, the effectiveness of AML/CFT measures depends on how well the executives and employees understand the policies, procedures, and programs. Financial institutions are required to ensure that employees have required expertise and qualifications through recruitment and training.

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

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 management and make it 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, clearly define the sequential processes of identifying, assessing, and mitigating the risks, taking into account the institution's size and characteristics.

In addition, a financial institution is required to evaluate the effectiveness of such policies, procedures, and programs, and revise them on an ongoing basis.

To evaluate the effectiveness of each process of identification, assessment, and mitigation of risks, it is important that executives responsible for and divisions in charge of AML/CFT conduct regular monitoring, while the internal audit division verifies how executives and employees of each division and branch are familiarized with the institution's AML/CFT measures.

Based on the result of this evaluation, a financial institution is required to reexamine possibilities of further improvements in the measures for each process and the management, and to enhance the policies, procedures, programs, and risk management for the identification, assessment, and mitigation of risks.

Required actions for a financial institution

A financial institution shall:

- 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.
- 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.
- iii. Assess the residual risk after taking risk mitigation measures, and examine the necessity for enhancing the risk mitigation measures and for implementing additional measures by the control division.
- iv. Have the control division and internal audit division evaluate the effectiveness of the risk management, taking into account internal information, whistle-blowing reports and questions from employees.
- v. If, as the result of the aforementioned evaluation of effectiveness, possibilities of further improvements are identified, enhance the policies, procedures, programs, and risk management, for the identification, assessment and mitigation of risks.

Expected actions for a financial institution

- A. Establish, as appropriate, a department solely dedicated to implementation of AML/CFT measures, taking account of the institution's size, characteristics, and business operations and other factors.
- B. Similarly, undergo a review by an external expert, as appropriate.

III-2 Involvement and understanding of management

The level of ML/FT risks faced by a financial institution varies according to the way it operates based on their business strategy. Therefore, ML/FT risks must be assessed in the context of the institution's business strategy, as part of the processes of evaluating and reviewing risk appetite and resource allocation policy.

As seen in the past cases involving large fines or termination of business relationship, failure to implement effective AML/CFT measures leads to a management problem such as reputational damage.

Furthermore, "tone at the top" is critical to increase the awareness of AML/CFT measures among the executives and employees including the business divisions. Management 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 the above, the management of financial institutions is required to consciously and proactively be engaged in AML/CFT and promote enhancement of the institution's AML/CFT measures.

Required actions for a financial institution

A financial institution shall:

- i. Recognize AML/CFT as one of the most important strategic issues.
- ii. Appoint an executive responsible for AML/CFT measures of the institution, granting the authority necessary to fulfill the responsibilities.
- 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 to internal and external stakeholders.
- iv. In view of the importance of AML/CFT, allocate adequate resources such as personnel with expertise and the sufficient budget to the division responsible for AML/CFT.
- v. Establish programs for coordination between the executives and divisions involved in AML/CFT.
- vi. Ensure that management participates or is otherwise proactively involved in AML/CFT training for management and employees.

Expected actions for a financial institution

- A. Ensure that an appraisal and remuneration systems appropriately reflects compliance records and contributions of executives and employees to AML/CFT measures.

III-3 Management and control: three lines of defense

Financial institutions are required to establish effective ML/FT risk management in accordance with the size and characteristics of their business operations. It is important that management takes responsibility for defining the roles and responsibilities of the business divisions, control and audit divisions in the fight against ML/FT, and implement measures in a coordinated manner.

One way of clarifying the roles and responsibilities of each division is defining the functions of business divisions, control and audit divisions under the concept of "three lines of defense."

In the following sections, the functions in the ML/FT risk management 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 management 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*.

(1) First line of defense

The first line of defense (“the first line”) is the business division. Branches and the business divisions that are engaged in business activities serving customers are the front line to face ML/FT risks first and therefore play a primary role in prevention of ML/FT.

In order for the first line to function effectively, all employees belonging to the first line must engage in day-to-day business operations with a correct understanding of ML/FT risks.

Financial institutions are required to take measures necessary to promote the first line’s understanding of the ML/FT risks associated with their operations, in light of the nature of such operations, for example, by formulating and disseminating AML/CFT policies, procedures, and programs, and by providing training to raise awareness.

Required actions for a financial institution

A financial institution shall:

- 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.
- 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.

(2) Second line of defense

The second line of defense (“the second line”) is control divisions such as compliance and risk management. The second line independently checks the autonomous risk controls by the first line, and at the same time supports the first line in implementing controls.

For the purpose of AML/CFT risk management, control divisions include the main division in charge of AML/CFT, the system division responsible for transaction monitoring systems, and the personnel division in charge of hiring and maintaining personnel with expertise.

In order to fulfill the roles for supporting and checking the first line, the control divisions are required to possess knowledge relating to business of the first line as well as correct understanding of the ML/FT risks inherent to the business.

Required actions for a financial institution

A financial institution shall:

- i. Monitor independently whether the ML/FT risk management 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.
- 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.
- 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.
- iv. Allocate employees with sufficient knowledge and expertise of AML/CFT to control divisions.

(3) Third line of defense

The third line of defense (“the third line”) is the internal audit division. The internal audit division is required to independently verify whether the first line and second line are functioning appropriately and whether there is any possibility for further enhancement on a regular basis.

In addition, the internal audit division is required to independently verify the effectiveness of firm-wide AML/CFT policies, procedures, and programs, and point out and advise on the necessity for reviewing the policies, procedures and programs or for enhancing the measures.

Required actions for a financial institution

A financial institution shall:

- i. Formulate an audit plan that includes the verification of the following items 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.

- ii. Ensure that the scope, frequency and approaches of audits are appropriate in light of the ML/FT risks being faced.
- 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.
- iv. Report the results of the internal audits conducted by the internal audit division to the corporate auditors and management, and follow up on the audit results and advise on improvements.
- v. Allocate employees with the sufficient knowledge and expertise of AML/CFT to the internal audit division.

III-4 Group-wide risk management

A financial institution that forms a financial group 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.

In particular, where a financial group operates through overseas offices, it is required to recognize the difference in the geographic, political, and other environments between Japan and the foreign jurisdictions and establish group-wide programs consistently applied across the group in consideration of such differences to ensure the effectiveness of the AML/CFT measures.

Moreover, it should be noted that differences in AML/CFT requirements and information protection regulations between Japan and foreign jurisdictions may make it difficult to share information necessary for effective implementation of AML/CFT measures.

Therefore, a financial group that operates through overseas offices is required to establish risk management 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.

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

Required actions for a financial institution

A financial institution shall:

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

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

Cases of advanced practices :

a case where a financial institution's head office conducts firm-wide risk identification and assessment that includes overseas offices applying a common approach, and determines the residual risk of each overseas office based on the actual situation identified by on-site reviews.

Specifically, the institution formulates an AML/CFT program applied to the entire group, including overseas offices, and based on the program, the head office division responsible for AML/CFT of the group centrally manages the information of each office including the number of accounts and the number of high-risk customers, and identifies and assesses the risks of each overseas office applying a common approach.

Then, the head office division assesses the effectiveness of mitigation measures of each office based on discussions, taking into account the factors such as the number of employees, the status of training, and the distinctive characteristics of IT and other infrastructure.

Furthermore, in order to deal with the residual risks after applying mitigation measures, the head office division in charge of AML/CFT conducts on-site reviews, and takes additional measures for the offices with a high level of residual risks, such as increasing the frequency of monitoring and audits.

Cases of advanced practices :

a case where a financial institution implements a centralized system for sharing information on a group-wide basis. The system enables the overseas offices to daily update and simultaneously share with the head office, customer information and transaction information obtained from their day-to-day operations.

III-5 Human resource development

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 management.

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 (including the acquisition of relevant qualifications) on an ongoing basis.

Required actions for a financial institution

A financial institution shall:

- 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.
- 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.

- 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.
- iv. Evaluate the effectiveness of training, for example, by checking the compliance with the requirements covered by the training or by providing employees with follow-up.
- 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.

Expected actions for a financial institution

- A. 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, provide training about the importance of risk assessment and the correct way of assessing risks, taking into account the unique and specific situation of such office, and review the contents of such training on an ongoing basis.
- B. Where a financial group operates through overseas offices and the overseas operations are strategically important for the institution, establish programs for supporting the employees in charge of AML/CFT measures to undergo effective training and obtain relevant qualifications in relation to international trends concerning ML/FT.

IV Monitoring and Public Private Partnership

IV-1 Monitoring by the Financial Services Agency

As noted earlier, the FSA effectively monitors AML/CFT measures that financial institutions undertake taking into account the Guidelines, shares the outcome from the monitoring with individual institutions and industries, urges them to enhance ML/FT risk management, and takes necessary supervisory actions.

The FSA focuses on substantive ML/FT risks. Therefore, the FSA collects and integrates available information to identify and assess the ML/FT risks of each business category and those of each individual financial institution in respective industries, with a holistic review of the financial system. Based on the assessment, the FSA conducts effective and efficient monitoring by allocating resources according to the level of the identified and

assessed ML/FT risks.

In the aforementioned processes of identifying and assessing ML/FT risks across and within business categories, the FSA considers the characteristics of financial institutions and business categories such as; the variety of products and services, transactions types, countries and geographic areas, and customer bases, as well as international trend relating to ML/FT. The FSA utilizes these factors to conduct forward-looking monitoring.

In order to conduct the aforementioned identification, assessment and analysis of ML/FT risks, objective data such as quantitative and qualitative information are necessary. The FSA further improves the effectiveness of its risk-based monitoring by collecting the below-listed information from financial institutions in addition to already available data, and conducting interviews or other qualitative researches about the internal control. In order to effectively conduct such monitoring, the FSA develops expertise of specialists including employees of the Local Finance Bureaus and increases the number of employees with expertise through further recruitment of external experts.

- ✓ Number of suspicious transaction reports filed (breakdown by country/geographic area, customer attribute, etc.);
- ✓ Implementation of internal audits and training (including relevant qualification status);
- ✓ Risk assessment sheet that a financial institution is required to prepare under the Criminal Proceeds Act ; and
- ✓ Reports to management on ML/FT risk management, and the records of discussions.

That information is also useful for a financial institution to conduct identification and assessment of its ML/FT risks under its risk-based approach. A financial institution is thus expected to accumulate, organize, and utilize information necessary for their risk analyses including information listed above to improve the effectiveness of its risk-based approach.

The FSA proactively shares cases collected through the monitoring process and information obtained from foreign authorities with financial institutions and industry associations to improve the overall level of AML/CFT of Japanese financial institutions.

Article 3, paragraph 3 of the Criminal Proceeds Act stipulates that the National Public Safety Commission publishes the Japanese NRA concerning the risks of transfer of criminal proceeds in Japan. The FSA, as the supervisory authority of financial institutions, monitors financial institutions with the risk-based approach, taking into account the NRA.

IV-2 Public private partnership and cooperation with relevant authorities

In order to address increasing ML/FT risks and ensure the entire soundness of Japan's financial system, it is necessary, in addition to the actions of individual financial

institutions, that relevant domestic and foreign authorities, industry associations, financial institutions, and other private companies coordinate and cooperate to address the ML/FT risks.

In particular, it is important to follow information on international discussions and advanced practices in order to swiftly address ever-changing ML/FT trends. However, that information may in some cases not be easily gathered by an individual financial institution, and thus information gathering by the individual institution may be inefficient for accumulating the knowledge to address the ML/FT risks.

In view of that, the FSA enhances information gathering through larger coordination with industry associations, relevant ministries and agencies, and foreign authorities, and shares with financial institutions good practices gathered through the coordination and the useful cases obtained through the monitoring. In addition to the coordination with business associations, the FSA engages in and undertakes ongoing dialog with individual financial institutions, in order to facilitate continuous examination of AML/CFT-related issues, solutions, and improvement among financial institutions and industries.

Meanwhile, industry associations need to play a central role in providing member financial institutions with information on the latest trends, issues and actual cases or possible solutions to address the issues, and overseas useful practices regarding AML/CFT, and in supporting the implementation and the improvement of AML/CFT for those financial institutions.

Furthermore, for improving the efficiency of ML/FT risk management, it is important to promote and enhance measures such as the introduction of new technologies and joint operation by outsourcing, in various areas such as CDD, risk assessment, and transaction monitoring and screening, besides information sharing as mentioned above.

At the same time, for further facilitating smooth communication between the public and the private sector, the FSA continues to review its approaches of monitoring and outreach reflecting discussions with industry associations and individual financial institutions.

These activities by the FSA need to be operated effectively in coordination with relevant ministries and agencies in Japan. In particular, monitoring on foreign remittances would be enhanced in its effectiveness and efficiency by coordination with the Ministry of Finance with respect to its foreign exchange inspections under the Foreign Exchange Act. It is also beneficial to exchange information and engage with foreign authorities.

In these ways, with proactive and close engagement and coordination with industry associations, individual financial institutions, relevant ministries and agencies, and foreign authorities, the FSA ensures effective AML/CFT in Japan.

| | |
|------------------|---------|
| February 6, 2018 | Issued |
| April 10, 2019 | Amended |