

Comprehensive Guidelines for Supervision of  
Financial Market Infrastructures

- Clearing Organizations, Fund Clearing Organizations,  
Book-entry Transfer Institutions, and Trade Repositories -

Text

June 2022

Financial Services Agency

# Comprehensive Guidelines for Supervision of Financial Market Infrastructures

## - Clearing Organizations, Fund Clearing Organizations, Book-entry Transfer Institutions, and Trade Repositories -

|  |    |
|--|----|
| I. Basic Concept   |    |
| I-1 Basic Concept for Supervision of Financial Market Infrastructures  | 1  |
| I-1-1 Purpose of Supervision of Financial Market Infrastructures and the Role of<br>Supervisory Departments                                | 1  |
| I-1-2 Basic Concept for Supervision of Financial Market Infrastructures  | 2  |
| I-2 Purpose of Establishment of the Guidelines for supervision   | 4  |
| I-2-1 Purpose of Establishment of the Guidelines for supervision   | 4  |
| I-2-2 Structure of the Guidelines  | 5  |
| II. Points to Consider regarding the Conduct of Administrative Processes Regarding the<br>Supervision of Financial Market Infrastructures  | 6  |
| II-1 General Administrative Processes, etc.  | 6  |
| II-1-1 General Supervisory Processes   | 6  |
| II-1-2 Cooperation with Inspection Departments   | 7  |
| II-1-3 Cooperation with Relevant Ministries/Agencies, the Bank of Japan and Foreign<br>Authorities   | 8  |
| II-2 Response to External Inquiries about Interpretations of Laws and Regulations,<br>etc.   | 9  |
| II-2-1 Inquiries about Laws and Regulations  | 9  |
| II-2-2 Prior Confirmation Procedures for the Application of Laws and Regulations by<br>Administrative Agencies (“No Action Letter” System) | 11 |
| II-2-3 System to Eliminate Regulatory Gray Zones   | 13 |
| II-3 Points to Consider when Providing Administrative Guidance, etc.   | 18 |
| II-3-1 Points to Consider when Providing Administrative Guidance, etc.   | 18 |
| II-3-2 Points to Consider when Holding Interviews, etc.  | 20 |
| II-4 Points to Consider when Taking Administrative Actions   | 22 |
| II-4-1 Clearing Organizations  | 22 |
| II-4-1-1 Response to Inspection Results, etc.  | 22 |
| II-4-1-2 Administrative Actions Based on Provisions of the FIEA (Business<br>Improvement Orders, Business Suspension Orders, etc.)         | 23 |
| II-4-1-3 Standard Processing Period  | 25 |
| II-4-1-4 Removal of the Requirement for the Submission of Reports on Compliance<br>with Business Improvement Orders                        | 25 |
| II-4-1-5 Relation to the Administrative Procedure Act and Other<br>Laws  | 26 |
| II-4-1-6 System for Exchange of Opinions   | 27 |
| II-4-1-7 Notification to Relevant Authorities, including Foreign Supervisory<br>Authorities  | 28 |

|           |   |    |
|-----------|---|----|
| II-4-1-8  | Concept on the Publication of Unfavorable Dispositions  | 28 |
| II-4-1-9  | Points for Attention Concerning Preparation of Documents Required to be Submitted by COs  | 28 |
| II-4-1-10 | Points of Attention Regarding Submitting Applications, etc. which can be filed electronically   | 28 |
| II-4-2    | Fund Clearing Organizations   | 30 |
| II-4-2-1  | Response to Inspection Results, etc.  | 30 |
| II-4-2-2  | Administrative Actions Based on Provisions of the Payment Services Act (Business Improvement Orders, Business Suspension Orders, etc.)    | 31 |
| II-4-2-3  | Standard Processing Period, etc.  | 33 |
| II-4-3    | Book-entry Transfer Institutions  | 33 |
| II-4-3-1  | Response to Inspection Results, etc.  | 33 |
| II-4-3-2  | Administrative Actions Based on Provisions of the Book-Entry Transfer Act (Business Improvement Orders, Business Suspension Orders, etc.) | 34 |
| II-4-3-3  | Standard Processing Period, etc.  | 36 |
| II-4-4    | Trade Repositories  | 36 |
| II-4-4-1  | Response to Inspection Results, etc.  | 36 |
| II-4-4-2  | Administrative Actions Based on Provisions of the FIEA (Business Improvement Orders, Business Suspension Orders, etc.)                    | 38 |
| II-4-4-3  | Standard Processing Period, etc.  | 39 |
| III.      | Supervisory Viewpoints and Procedures (Clearing Organizations)  | 40 |
| III-1     | Governance / Business Administration  | 40 |
| III-1-1   | Governance System   | 40 |
| III-1-2   | Officers of Clearing Organizations  | 44 |
| III-1-3   | Staffing  | 44 |
| III-2     | Financial Soundness   | 47 |
| III-2-1   | Adequacy of Capital   | 47 |
| III-2-2   | Comprehensive Risk Management Framework   | 48 |
| III-2-3   | Credit Risk Management  | 49 |
| III-2-4   | Liquidity Risk Management   | 51 |
| III-2-5   | Margin System   | 52 |
| III-2-6   | Collateral System   | 54 |
| III-2-7   | Development of Recovery Plans   | 55 |
| III-2-8   | Supervisory Method and Actions  | 57 |
| III-3     | Operational Appropriateness   | 58 |
| III-3-1   | Compliance  | 58 |
| III-3-1-1 | Measures for Ensuring Compliance  | 58 |
| III-3-1-2 | Fair Participation Requirements, etc.   | 58 |
| III-3-1-3 | Prevention of Damage that May be Inflicted by Anti-Social Forces  | 59 |
| III-3-2   | Business Continuity Management (BCM)  | 64 |

|   |     |
|---|-----|
| III-3-3 Operational Risk Management   | 66  |
| III-3-4 Information Technology Risk Management                              | 68  |
| III-3-5 Procedures to Deal with Participant Default, etc.                   | 76  |
| III-3-6 Management and Investment of Collateral, etc.                       | 77  |
| III-3-7 Notes concerning Tiered Structure of Participants, etc.             | 79  |
| III-3-8 Appropriateness of Disclosure of Information, etc.                  | 80  |
| III-4 Administrative Procedures   | 82  |
| III-4-1 Points to Consider regarding Authorization of Business Rules, etc.  | 82  |
| III-4-2 Points to Consider regarding Approval of Subsidiary Business        | 83  |
| IV. Supervisory Viewpoints and Procedures (Fund Clearing Organizations)     | 85  |
| IV-1 Governance / Business Administration                                   | 85  |
| IV-1-1 Governance System  | 85  |
| IV-1-2 Officers of Fund Clearing Organizations                              | 89  |
| IV-1-3 Staffing   | 90  |
| IV-2 Financial Soundness  | 92  |
| IV-2-1 Adequacy of Capital  | 92  |
| IV-2-2 Comprehensive Risk Management Framework                              | 93  |
| IV-2-3 Credit Risk Management   | 94  |
| IV-2-4 Liquidity Risk Management  | 95  |
| IV-2-5 Collateral System  | 96  |
| IV-2-6 Supervisory Method and Actions                                       | 97  |
| IV-3 Operational Appropriateness  | 98  |
| IV-3-1 Compliance   | 98  |
| IV-3-1-1 Measures for Ensuring Compliance                                   | 98  |
| IV-3-1-2 Fair Participation Requirements, etc.                              | 98  |
| IV-3-1-3 Prevention of Damage that May be Inflicted by Anti-Social Forces   | 99  |
| IV-3-2 Business Continuity Management (BCM)                                 | 104 |
| IV-3-3 Operational Risk Management  | 106 |
| IV-3-4 Information Technology Risk Management                               | 107 |
| IV-3-5 Procedures to Deal with Participant Default, etc.                    | 116 |
| IV-3-6 Management of Collateral, etc.                                       | 117 |
| IV-3-7 Notes concerning Tiered Structure of Participants, etc.              | 118 |
| IV-3-8 Appropriateness of Disclosure of Information, etc.                   | 119 |
| IV-4 Various Administrative Procedures                                      | 120 |
| IV-4-1 Points to Consider regarding Authorization of Business Rules, etc.   | 120 |
| IV-4-2 Points to Consider regarding Approval of Subsidiary Business         | 121 |
| V. Supervisory Viewpoints and Procedures (Book-entry Transfer Institutions) | 123 |
| V-1 Governance / Business Administration                                    | 123 |
| V-1-1 Governance System   | 123 |
| V-1-2 Officers of Book-entry Transfer Institutions                          | 127 |

|  |     |
|--|-----|
| V-1-3 Staffing   | 128 |
| V-2 Financial Soundness  | 130 |
| V-2-1 Adequacy of Capital  | 130 |
| V-2-2 Risk Management Framework  | 131 |
| V-2-3 Supervisory Method and Actions   | 132 |
| V-3 Operational Appropriateness  | 133 |
| V-3-1 Compliance   | 133 |
| V-3-1-1 Measures for Ensuring Compliance   | 133 |
| V-3-1-2 Fair Participation Requirements, etc.  | 133 |
| V-3-1-3 Prevention of Damage that May be Inflicted by Anti-Social Forces                 | 134 |
| V-3-1-4 Verification at the Time of Transaction and Reporting of Suspicious Transactions | 139 |
| V-3-2 Business Continuity Management (BCM)   | 142 |
| V-3-3 Operational Risk Management  | 144 |
| V-3-4 Information Technology Risk Management   | 145 |
| V-3-5 Procedures to Deal with Default of AMIs, etc.                                      | 154 |
| V-3-6 Notes concerning Tiered Structure of Participants, etc.                            | 155 |
| V-3-7 Appropriateness of Disclosure of Information, etc.                                 | 155 |
| V-4 Administrative Procedures  | 157 |
| V-4-1 Points to Consider regarding Authorization of Business Rules, etc.                 | 157 |
| V-4-2 Points to Consider regarding Approval of Subsidiary Business                       | 157 |
| VI. Supervisory Viewpoints and Procedures (Trade Repositories)                           | 160 |
| VI-1 Governance / Business Administration  | 160 |
| VI-1-1 Governance System   | 160 |
| VI-1-2 Officers of Trade Repositories  | 164 |
| VI-1-3 Staffing  | 164 |
| VI-2 Financial Soundness   | 167 |
| VI-2-1 Adequacy of Capital   | 167 |
| VI-2-2 Risk Management Framework   | 168 |
| VI-2-3 Supervisory Method and Actions  | 169 |
| VI-3 Operational Appropriateness   | 170 |
| VI-3-1 Compliance  | 170 |
| VI-3-1-1 Measures for Ensuring Compliance  | 170 |
| VI-3-1-2 Fair Access Requirements, etc.  | 170 |
| VI-3-1-3 Prevention of Damage that May be Inflicted by Anti-Social Forces                | 171 |
| VI-3-2 Business Continuity Management (BCM)  | 176 |
| VI-3-3 Operational Risk Management   | 177 |
| VI-3-4 Information Technology Risk Management  | 178 |
| VI-3-5 Appropriateness of Disclosure of Information, etc.                                | 187 |
| VI-3-5-1 Disclosure of Major Rules, etc.   | 187 |

|   |     |
|---|-----|
| VI-3-5-2 Disclosure of Market Data  | 188 |
| VI-4 Administrative Procedures  | 190 |
| VI-4-1 Points to Consider regarding Authorization of Business Rules, etc. | 190 |
| VI-4-2 Points to Consider regarding Approval of Subsidiary Business       | 191 |

## **I. Basic Concept**

### **I-1 Basic Concept for Supervision of Financial Market Infrastructures**

#### **I-1-1 Purpose of Supervision of Financial Market Infrastructures and Role of Supervisory Departments**

Clearing Organizations (COs) (meaning Financial Instruments Clearing Organizations prescribed in Article 2(29) of the FIEA; the same shall apply hereinafter), Foreign Financial Instruments Clearing Organizations (FFICOs) (meaning the Foreign Clearing Organizations prescribed in that paragraph; the same shall apply hereinafter), Fund Clearing Organizations (FCOs) (meaning Fund Clearing Organizations prescribed in Article 2(11) of the PSA; the same shall apply hereinafter), Book-entry Transfer Institutions (BeTIs) (meaning Book-entry Transfer Institutions prescribed in Article 2(2) of the Book-Entry Transfer Act; the same shall apply hereinafter) and Trade Repositories (TRs) (meaning Trade Repositories prescribed in Article 156-64(3) of the FIEA; the same shall apply hereinafter) (hereinafter collectively referred to as “financial market infrastructures”) perform a huge quantity and amount of post-trade processes for financial transactions of securities, etc. such as clearing, book-entry transfer, and recording.

(Note) FIEA: Financial Instruments and Exchange Act

PSA: Payment Services Act

Book-Entry Transfer Act: Act on Book-Entry Transfer of Company Bonds, Shares, etc. (the same shall apply hereinafter)

The performance of a huge quantity and amount of post-trade processes by financial market infrastructures enables their participants, etc. to carry out operations in an effective and efficient manner, and reduce the risks involved in financial transactions.

On the other hand, once a problem arises in the operations of financial market infrastructures, there is a possibility that participants, etc. will face serious risks due to the concentrated processing of transactions in large quantities and amounts. Also, in the event of loss of confidence in the soundness, etc. of financial market infrastructures that perform transactions, etc. in large quantities and amounts with numerous parties, unexpected turmoil in the financial system may be induced.

For this reason, it is important for financial market infrastructures to properly execute clearing, book-entry transfer, recording and other such operations and to conduct appropriate risk management in view of ensuring confidence in them, and in turn, ensuring the stability of Japan’s financial system.

The purpose of supervision of financial market infrastructures is to ensure the sound and

appropriate operations of financial market infrastructures, thereby contributing to enhanced financial stability and investor protecting in Japan.

In order to conduct administrative supervision in an effective manner, it is necessary to properly combine the “on-site” monitoring conducted by inspection departments that inspect financial market infrastructures and the “off-site” monitoring conducted by supervisory departments. In addition, in order to enhance the effectiveness of supervision, inspection and supervisory departments need to exercise their respective functions properly while maintaining appropriate cooperation.

The role of supervisory departments under this framework is to promptly identify problems that may affect the soundness and appropriateness of the operations of financial market infrastructures through continual collection and analysis of information, while encouraging improvements. To be more specific, the key role is to promptly identify problems and encourage financial market infrastructures to make improvements through periodic and continuous exchanges of opinions and other means, as well as the accumulation and analysis of various data and information provided by them.

### **I-1-2 Basic Concept for Supervision of Financial Market Infrastructures**

In light of the above, the basic concept for the supervision of financial market infrastructures can be described as follows:

#### **(1) Appropriate Cooperation with Inspection Departments**

It is important for supervisory and inspection departments to properly cooperate with each other while respecting each other’s independence, and to achieve highly effective supervision of financial market infrastructures, by properly combining both on-site and off-site monitoring. To this end, supervisory departments shall pay due consideration to the following points regarding cooperation with inspection departments.

- (i) Supervisory departments shall conduct follow-up monitoring of improvements concerning the problems identified by inspections and strive to ensure that the problems are corrected. They shall take strict supervisory measures, including administrative actions, when necessary.
- (ii) The problems identified by supervisory departments through off-site monitoring shall be notified to inspection departments as feedback for use in the next inspection.

#### **(2) Securing Sufficient Communication with Financial Market Infrastructures**

In the supervision of financial market infrastructures, it is important to precisely grasp



and analyze information concerning their business management and use the analysis results for supervisory activities as necessary in an appropriate and timely manner.

Therefore, rather than merely waiting for reports from financial market infrastructures, supervisory authorities need to proactively gather information through day-to-day communication with them. To be more specific, supervisory authorities need to ensure daily communication with financial market infrastructures, through periodic exchanges of opinions with them and other such means, so as to grasp information not only concerning their financial conditions, but also various business management matters.

### **(3) Respect of Voluntary Efforts by Financial Market Infrastructures**

The standpoint of supervisory authorities is to examine, in light of laws and regulations, the state of the series of functions provided directly by financial market infrastructures pursuant to laws and regulations, and management decisions made by them based on the principle of self-responsibility, and to encourage correction of problems. With due consideration of this standpoint, supervisory authorities shall respect the voluntary efforts of financial market infrastructures regarding business operations when supervising them.

### **(4) Securing Efficient and Effective Supervisory Processes**

In order to make effective use of the limited resources of the supervisory authorities as well as those of financial market infrastructures, it is necessary to implement supervisory processes in an efficient and effective manner. Therefore, when requiring financial market infrastructures to submit reports and other materials, supervisory authorities should make sure to limit the volume of the required reports and materials to the minimum necessary for the supervisory purpose and strive to improve the efficiency of supervision by, for example, constantly reviewing the necessity of existing supervisory processes and the method of implementing them and by making improvements as necessary.

## **I-2 Purpose of Establishment of the Guidelines for Supervision**

### **I-2-1 Purpose of Establishment of the Guidelines for Supervision**

In Japan's settlement system, operations conducted by financial market infrastructures have become increasingly broad and complex ever since the Financial System Council released a report titled "Reform of securities settlement systems toward the 21st century" in 2000, as reflected in the dematerialization of corporate bonds, government bonds, etc. and the development of the clearing organization system in 2002, the dematerialization of stock certificates in 2009, and the introduction of the obligation to store clearing and transaction information of over-the-counter (OTC) derivatives in 2012.

Furthermore, the international regulatory environment has also been changing dramatically for financial market infrastructures: for example, the Committee on Payment Settlement Systems (CPSS)<sup>(Note)</sup> of the Bank for International Settlements (BIS) and the International Organization of Securities Commissions (IOSCO) conducted a comprehensive review of international standards on existing payment systems, securities settlement systems and central counterparties (CCPs) in consideration of such matters as the lessons learnt from the recent financial crisis, and formulated and announced the "Principles for Financial Market Infrastructures (PFMIs)", which sought to integrate and enhance these standards.

(Note) The Committee on Payment and Settlement Systems (CPSS) changed its name to the Committee on Payments and Market Infrastructures (CPMI) on September 1, 2014.

Under these circumstances, it is decided to formulate these Guidelines in order to clarify the viewpoints, methods, etc. of supervision of financial market infrastructures in consideration of the new international standards and effectively conduct daily supervisory processes, and thereby ensure that business operations of financial market infrastructures shall be conducted more appropriately.

These Guidelines were compiled with due consideration of the actual state of financial market infrastructures, so that they can be applied to various cases, and the requirements of the supervisory viewpoints specified in the Guidelines shall not be rigidly applied to all financial market infrastructures

Accordingly, when applying these Guidelines, it should be noted that even when a requirement of all viewpoints is not met in a word-by-word literal manner, it would not necessarily be judged inappropriate insofar as there is no problem from the viewpoint of protecting public interests and investors; it is necessary to avoid applying the Guidelines in an absolute and uniform fashion. On the other hand, it should also be noted that there would be cases when there is room for improvement from the viewpoint of protecting public interests

and investors even if requirements of viewpoints are sufficiently fulfilled.

Clearing operations that can be performed by a financial instruments exchange by obtaining approval from the Prime Minister (Article 156-19(1) of the FIEA) are also subject to the same regulations as COs under the FIEA and are within the scope of these Guidelines.

For the book-entry transfer of government bonds, there is a special provision under which the Bank of Japan (BOJ) can be specified as the entity engaged in book-entry transfer operations (Article 47(1) of the Book-Entry Transfer Act). When conducting supervision on the BOJ as the entity engaged in book-entry transfer operation with Guidelines, the peculiarity of the organization of the BOJ—which is managed under the Bank of Japan Act—shall be taken into account, and due consideration shall be given to its autonomy in business operations.

With this in mind, supervisory departments shall execute supervisory processes for financial market infrastructures under these Guidelines.

### **I-2-2 Structure of the Guidelines**

These Guidelines were structured so that they can be used effectively for the supervision of financial market infrastructures.

“I. Basic Concept” and “II. Basis upon the Conduct of Administrative Processes Regarding the Supervision of Financial Market Infrastructures” are applicable to all financial market infrastructures unless specified otherwise, and “Evaluation and Administrative Procedures on Supervision” for financial market infrastructures are sorted on a business-by-business basis from III. to VI.

The provisions provided in I. to III. with respect to COs are to apply *mutatis mutandis* to FFICOs, and examinations, etc. will be made with respect to FFICOs, by replacing certain terms as needed with due consideration of the actual status of operations based on the purpose of these Guidelines.

## **II. Points to Consider regarding the Conduct of Administrative Processes Regarding the Supervision of Financial Market Infrastructures**

### **II-1 General Administrative Processes, etc.**

#### **II-1-1 General Supervisory Processes**

##### **(1) Periodic Hearings**

As part of off-site monitoring activities, supervisory departments shall, in principle, hold periodic hearings with financial market infrastructures as follows.

##### **(i) Hearings Regarding Financial Results**

Supervisory departments shall hold hearings regarding the financial results of financial market infrastructures as well as problems with their financial positions in each accounting period. If quarterly disclosures are performed, supervisory departments shall hold hearings regarding quarterly financial results as necessary.

##### **(ii) Comprehensive Hearings**

Supervisory departments shall hold hearings at least once a year to identify the management plans and policies for business expansion, management of various risks, profit management, governance status, etc. of financial market infrastructures in a comprehensive manner. Senior officials of supervisory authorities shall hold hearings with top managers of financial market infrastructures as necessary.

##### **(iii) Hearings Regarding Risk Management**

Supervisory departments shall hold hearings at least once a year regarding the current state, issues and directions of risk management by financial market infrastructures. In doing so, supervisory departments shall also ask the top managers about such matters as their recognition of risk management and their state of involvement in risk management. Hearings shall also be conducted in regards to the risk management status as necessary, taking market trends and other such factors into account.

##### **(2) Hearings on an Ad-hoc Basis**

As part of off-site monitoring activities, supervisory departments shall hold hearings with financial market infrastructures, when it is deemed necessary to do so from the supervisory viewpoint due to factors such as changes in their business performance and strategies, or changes in the environment surrounding the system, and incidents that could undermine their sound and appropriate management.

Furthermore, supervisory departments shall bear in mind that the PFMI have been

formulated as international principles regarding the objectives of financial market infrastructures to be observed by them, and as necessary, hold hearings with financial market infrastructures on their status such as their compliance with the PFMIIs.

## **II-1-2 Cooperation with Inspection Departments**

It is important for supervisory and inspection departments to properly cooperate with each other while respecting each other's independence, and to achieve highly effective supervision by properly combining both on-site and off-site monitoring. To this end, supervisory departments shall pay due consideration to the following points regarding cooperation with inspection departments.

### **(1) Feedback of Information Regarding Problems and Issues Identified through Off-site Monitoring to Inspection Departments**

Feedback on problems and issues of financial market infrastructures identified by supervisory departments through off-site monitoring shall be provided to inspection departments for use in the next inspection.

Specifically, supervisory departments shall provide inspection departments with explanations concerning their current state, etc. with regard to the following matters before the inspection, for example:

- (i) Major moves made by financial market infrastructures since the previous inspection (e.g., business alliances with other companies, capital increases, management reshuffles)
- (ii) The schedule of system updates, etc. in the case of financial market infrastructures planning system updates, etc.
- (iii) The most recent financial results
- (iv) Results of comprehensive hearings
- (v) Status of the implementation of supervisory measures (e.g., requirements for the submission of reports and administrative actions) and follow-up thereon
- (vi) Matters which supervisory departments believe are important
- (vii) Other matters

### **(2) Supervisory Response to Problems and Issues Identified through Inspections**

Regarding inspections of financial market infrastructures conducted by inspection departments, supervisory departments shall consider taking necessary measures based on II-4 in order to properly reflect the inspection results in supervisory processes.

## **II-1-3 Cooperation with Relevant Ministries/Agencies, the Bank of Japan and Foreign Authorities**

### **(1) Cooperation among Relevant Ministries/Agencies**

The book-entry transfer system can be facilitated by making it adequately function at both the financial business practice level and the legal level in relation to the issuance, transfer, etc. of corporate bonds and other securities. In addition, the book-entry transfer system handles government bonds, etc., and BeTIs are within the joint jurisdiction of the FSA, the Ministry of Justice (MOJ) and the Ministry of Finance (MOF).

In light of the above, close cooperation shall be sought with the FSA, MOJ and MOF, such as sharing information and exchanging opinions as necessary, in cases where it is deemed appropriate to do so from a supervisory viewpoint, including cases where administrative disposition is to be taken or license/approval, etc. is to be granted with respect to BeTIs.

### **(2) Cooperation with the Bank of Japan**

In view of ensuring the facilitation of money settlements between financial institutions, the BOJ conducts *oversight* with respect to financial market infrastructures.

In light of the above, close cooperation shall be sought with the BOJ, such as sharing information and exchanging opinions as necessary, in cases where it is deemed appropriate to do so from a supervisory viewpoint, including cases where administrative disposition is to be taken or license/approval, etc. is to be granted with respect to financial market infrastructures.

### **(3) Cooperation with Foreign Authorities**

Among financial market infrastructures, international activities and other such developments are observed; for example, foreign financial institutions, etc. have become participants, and there are participants that have a foreign parent.

In light of the above, close cooperation shall be sought with foreign supervisory authorities, etc., such as sharing information and exchanging opinions as necessary, in cases where it is deemed appropriate to do so from a supervisory viewpoint, including cases where administrative disposition is to be taken or license/approval, etc. is to be granted with respect to financial market infrastructures

## **II-2 Response to External Inquiries about Interpretations of Laws and Regulations, etc.**

### **II-2-1 Inquiries about Laws and Regulations**

#### **(1) Scope of Laws and Regulations Regarding Which Inquiries May be Processed**

Inquiries may be processed only regarding the FIEA, the PSA, the Book-Entry Transfer Act and related laws, and regulations that are under the FSA's jurisdiction. Comments shall never be made in response to inquiries regarding laws and regulations outside the FSA's jurisdiction.

#### **(2) Response to Inquiries**

- (i) Regarding an inquiry to which a reply can be made based on existing documents and reference materials, such as these Guidelines and reports compiled by advisory councils, the reply shall be provided promptly.
- (ii) When business operators to which the laws and regulations under the FSA's jurisdiction are directly applicable or business associations<sup>Note</sup> comprising such business operators have made a general inquiry that meets the requirements specified in the following A and B with regard to the said laws and regulations, the head of the relevant FSA division shall provide a written reply and make it public if it is deemed to be appropriate to do so from the viewpoint of improving the predictability of the application of laws and regulations.

(Note) A "business association" refers to a group formed by a substantial number of business operators engaging in the same type of business to which the laws and regulations under the FSA's jurisdiction are directly applicable in order to promote their common interests, or a federation of such groups (limited to the top-tier organization in the case of business sectors where there are layers of associations and federations).

#### **A. Scope of Inquiries for Which the Reply may be Published**

An inquiry must meet all of the following requirements if the written reply thereto is to be made public:

- a. Must not ask whether a law or regulation is applicable to a specific transaction involving a specific business operator, but rather ask about the general interpretation of the law or regulation. (Not eligible for the application of the Prior Confirmation Procedures on the Application of Laws and Regulations by Administrative Agencies ("no action letter" system).)
- b. Must not seek factual recognition.

- c. Must relate to transactions and other matters common to business operators to which the laws and regulations under the FSA's jurisdiction are directly applicable (in cases where the inquirer is an association of business operators, the inquiry must concern transactions and other matters common to business operators constituting the association) and must be regarding matters that a number of business operators are expected to make an inquiry into.
- d. Must not ask about points that are clear in light of the Guideline for Administrative Processes and other documents and materials that have been made public in the past.

**B. Written Inquiry Forms (including Electronic Forms)**

The inquirer shall submit a written inquiry that specifies the following items. In addition to the written inquiry, the inquirer may be asked to submit additional or corrected documents, if necessary, in order to judge the contents of the inquiry and whether it meets the criteria specified in "A" above.

- a. The legal provision which the inquiry concerns and specific points of issue
- b. The inquirer's opinion concerning the inquired points of issue and the basis thereof
- c. A statement from the inquirer agreeing to have the contents of the inquiry and the response thereto made public.

**C. Contact Point for Inquiry**

A written inquiry shall be submitted to the FSA division with jurisdiction over the law or regulation in question.

**D. Reply**

- a. The head of the relevant FSA division shall strive to reply to the inquirer within two months in principle of the arrival of a written inquiry at the contact point. In cases where it is not possible to reply within two months, it is necessary to provide the reason for the delay and the expected date of reply to the inquirer.
- b. Written replies shall contain the following disclaimer:

"This reply expresses a general view regarding the law or regulation in question that the FSA formed at this time exclusively on the basis of information contained in the written inquiry, in its capacity as the entity that has jurisdiction over the said law or regulation. Therefore, the reply does not provide judgment regarding the application of the said law or regulation to a specific case or have binding power on the judgment of the investigative or judicial authorities."

- c. When the relevant FSA division decides not to reply to the inquiry through said process, it shall notify the inquirer of the decision and provide the basis thereof.

**E. Publication**



When the FSA has provided a reply according to the procedures prescribed in “D” above, it shall immediately publish the inquiry and the reply on its web site.

- (iii) Regarding inquiries which do not fit the description of (ii) above but are made frequently, a reference circular that describes the reply to the inquiry shall be compiled, distributed to the relevant departments and stored at the relevant departments of the FSA.
- (iv) In cases where the inquirer seeks a written reply from the FSA and where the Prior Confirmation Procedures on the Application of Laws and Regulations by Administrative Agencies (“no action letter” system) are applicable in light of II-2-2(2), the inquirer shall be asked to apply for the said procedures.

## **II-2-2 Prior Confirmation Procedures for the Application of Laws and Regulations by Administrative Agencies (“No Action Letter” System)**

Under the Prior Confirmation Procedures for the Application of Laws and Regulations by Administrative Agencies (hereinafter referred to as the “No Action Letter System”), private companies seek prior confirmation as to whether specific practices related to their planned business activities are subject to specific laws and regulations, and the said organizations make the replies they receive public. The FSA has established detailed rules concerning the No Action Letter System. This section only specifies the administrative procedures concerning the No Action Letter System, so supervisory departments shall make sure to refer to “Detailed Rules concerning the Prior Confirmation Procedures on the Application of Laws and Regulations by Administrative Agencies” when using the No Action Letter System.

### **(1) Contact Point for Inquiry**

Inquiries shall be submitted to the Supervisory Coordination Division of the Supervisory Bureau.

The Supervisory Coordination Division of the Supervisory Bureau shall immediately process the inquiry if it meets the requirements specified in (2) (iii) below and forward it to the division that has jurisdiction over the law or regulation in question.

### **(2) Flow of Processes after Receipt of a Written Inquiry**

The relevant division that has received the inquiry shall check whether it is appropriate to reply thereto in light of (i) and (iii) below in particular. In cases where the inquiry is not eligible for the No Action Letter System, the inquirer shall be notified of the ineligibility. In cases where it is deemed to be necessary for the inquirer to submit additional or corrected documents, the inquirer may be asked to do so. However, it is

important to avoid imposing an excessive burden on the inquirer, by minimizing the volume of requested additional or corrected documents.

**(i) Scope of Matters Subject to Inquiry**

Whether the inquiry has been submitted by a private company planning to engage in a new business or transaction in order to inquire about the following matters, in relation to the laws and ordinances listed on the FSA's website as subject to the No Action Letter System (hereinafter referred to as "Relevant Laws and Regulations (Provisions)") and government orders based thereon.

- A. Whether engaging in the business or transaction in question amounts to operating without authorization.
- B. Whether engaging in the business or transaction in question amounts to operating without notification.
- C. Whether engaging in the business or transaction in question leads to the suspension of business operation or rescission of a license (unfavorable dispositions).
- D. Whether engaging in the business or transaction in question leads to the direct imposition of a certain obligation or limitation of rights.

**(ii) Scope of Eligible Inquirers**

Whether the inquirer is an individual or a legal person planning to start a new business and wishing to inquire about the applicability of the Relevant Laws and Regulations (Provisions), or a lawyer or the like employed by the said individual or legal person. Whether the inquirer has submitted a written inquiry that meets the criteria specified in (iii) below and agreed to have the content of the inquiry and the reply thereto made public.

**(iii) Inquiry Content**

Written inquiry (including Electronic Forms) must meet the following criteria:

- A. Describing specific and concrete facts relating to planned business activity.
- B. Containing specific indication of the provisions of the Relevant Laws and Regulations (Provisions) regarding which the inquirer wishes to check the applicability to the planned activity.
- C. Containing a statement from the inquirer agreeing to have the contents of the inquiry and the reply thereto made public.
- D. Clarifying the inquirer's opinion concerning the applicability of the provisions of the laws and regulations in "B" above and the basis thereof.

**(iv) Response Timeframe**

In principle, the head of the division that has received the inquiry shall reply to the inquirer within 30 days from the arrival at the contact point of a written inquiry from the

inquirer. However, in the following cases, the response timeframe shall be set as follows.

In any case, the FSA shall strive to ensure that the response time, including the time needed for submitting additional or corrected documents, is made as short as possible.

A. In cases where the inquiry concerns advanced financial techniques or technologies, thus requiring a careful judgment, the FSA shall make a reply within 60 days in principle from the receipt of the inquiry.

B. In cases where the relevant section's conduct of administrative processes may be impeded significantly by an excessive volume of inquiries, a reply may be delayed till 30 days from the initial receipt of the inquiry or later but must be made within a reasonable period of time.

C. In cases where the law or regulation in question is under the joint jurisdiction of the FSA and another government agency, a reply shall be made within 60 days in principle from the receipt of the inquiry.

In cases where the inquirer has been asked to submit corrected or additional information, the days involved in gathering the said information shall not be counted in the 30-day period. If it is not possible to make a reply within 30 days, the FSA shall provide the reason for the delay and the expected date of reply to the inquirer.

**(v) Publication of Inquiries and Replies**

As a general rule, the contents of inquiries and the replies thereto shall be posted on the FSA's website in their entirety within 30 days from the issuance of the reply.

However, in cases where the inquirer requests a delay in the publication of the inquiry and the reply thereto, and provides a rational reason for the delay and specifies the time when publication may be made, the FSA may delay the publication of the inquiry and the reply. In such cases, the publication may not necessarily be delayed until the date requested by the inquirer. When the reason for the requested delay ceases to be valid, the FSA may make the inquiry and the reply thereto public after giving prior notice to the inquirer.

In cases where an inquiry or the reply thereto contains information that falls under the category of matters of non-disclosure, as specified under the provisions of Article 5 of the Act Concerning the Disclosure of Information Retained by Administrative Agencies, the FSA may, as necessary, withhold such information from disclosure.

**II-2-3 System to Eliminate Regulatory Gray Zones**

Article 9(1) of the Industrial Competitiveness Enhancement Act (hereinafter referred to as the

“Enhancement Act”) stipulates a system under which persons who intend to conduct new business activities may request confirmation of the interpretation of provisions of the law that stipulates regulations concerning the intended new business activities and related business activities, as well as ordinances based on the law (including notifications; hereinafter referred to as the “laws and ordinances” in this paragraph), and the presence or absence of application of said provisions to the new business activities and related activities (hereinafter referred to as the “Gray Zone Elimination System”). This paragraph prescribes the administrative processes of the Gray Zone Elimination System. Reference shall invariably be made to the “Guide to the Use of the ‘Special System for Corporate Field Tests’ and the ‘Gray Zone Elimination System’ of the Industrial Competitiveness Enhancement Act” (Ministry of Economy, Trade and Industry, January 20, 2014) formulated by the Ministry of Economy, Trade and Industry (hereinafter referred to as the “Usage Guide” in this paragraph).

(1) Contact point for inquiry

The contact point for inquiry shall be the Strategy Development Division, the Strategy Development and Management Bureau of the FSA.

The Strategy Development Division, the Strategy Development and Management Bureau of the FSA, which is the contact point for inquiry, shall promptly accept any inquiry form or copy thereof that satisfies the requirements indicated in the criteria for items to be included of (2)(iii) below when it arrives. If the laws and ordinances related to the request for confirmation described in said inquiry form are under the jurisdiction of the head of another relevant administrative organ, confirmation shall be requested without any delay to the said head of the relevant administrative organ.

(2) Procedures Following the Receipt of Inquiry Form

After accepting an inquiry form, the Strategy Development Division, the Strategy Development and Management Bureau shall promptly forward said inquiry form to the responsible section that has jurisdiction over the laws and ordinances related to the request for confirmation described in the inquiry form. While discussing with said responsible section, the Policy and Legal Division, Planning and Coordination Bureau shall check the following (i) through (iii) in particular regarding whether or not a response shall be given to the matter, and in the case of a request for confirmation that cannot use the System, the person who submitted said inquiry form (hereinafter referred to as the “submitter” in this paragraph) shall be thus notified. In addition, if any corrections to the inquiry form or submission of additional documents are necessary, the required responses may be requested of the submitter. However, additional documents shall be limited to the minimum to avoid excessive burden on the submitter. In the case where a request concerning laws and ordinances under the jurisdiction of the FSA has been

received as the head of the relevant administrative organ set forth in Article 9(3) of the Enhancement Act, pursuant to provisions thereof, the above notification and request for required responses shall be made to the relevant minister in charge set forth in the same paragraph.

**(i) Subject of the Request for Confirmation**

Whether A. and B. below are satisfied.

A. Whether the submitter is a person who intends to conduct new business activities.

(Note) “New business activities” refer to the development or production of new products, the development or provision of new services, the introduction of new production or sales methods of products, the introduction of new provision methods of services and other new business activities through which improvement of productivity (including resource productivity (the degree of the contribution of the use of energy or the use of mineral resources (excluding their use as energy) to the economic activities of those who intend to conduct new business activities)) or cultivation of new demand is expected and which have no danger of injuring public order or morals (Article 2(3) of the Enhancement Act; Article 2 of the Ordinance for Enforcement of the Enhancement Act).

B. Whether the submitter is a person who intends to conduct new business activities related to businesses under the jurisdiction of the FSA. However, this shall not apply to cases where the Commissioner of the FSA has received a request as the head of the relevant administrative organ set forth in Article 9(3) of the Enhancement Act, pursuant to provisions thereof.

**(ii) Subject of the Inquiry**

Whether the submitter requests confirmation of the interpretation of provisions of the laws and ordinances under the jurisdiction of the FSA that stipulate regulations concerning the new business activities and related business activities the submitter intends to conduct, as well as the presence or absence of application of said provisions, and inquires on matters such as the following:

A. Whether conducting the business or transaction constitutes a business which can be conducted by a person who has received a license or designation.

B. Whether conducting the business or transaction constitutes a business requiring approval.

C. Whether conducting the business or transaction would be subject to suspension of business or rescission of license or designation (adverse disposition).

D. Whether obligations will be directly imposed or rights be restricted in relation to the conduct of the business or transaction.

**(iii) Criteria for Items to be Included in the Inquiry Form**

Whether the following matters are included in accordance with Form 5 of the Ordinance for Enforcement of the Enhancement Act and based on the Usage Guide.

- A. The goals of the new business activities and related business activities
- B. The particulars of the new business activities and related business activities
- C. Timing of conducting the new business activities and related business activities
- D. Clauses of the laws and ordinances for which confirmation of interpretation and presence or absence of application are requested
- E. Specific matters to be confirmed

(Reference) Usage Guide

Gray Zone Elimination System

Documents to be submitted

5. Specific matters to be confirmed

Describe the provisions of the laws and ordinances that are the basis of the regulations and the interpretation of which points thereof are unclear, as well as the points where it cannot be determined whether the new business activities would be subject to the regulations. Also state the reason that conducting the new business activities would be difficult due to such points and your own views concerning the matter.

In order to gain a clear and straight-forward response from the ministries that have jurisdiction over the regulations, describe the points you wish to confirm as specifically as possible, such as, “Since it is not clear whether xx is subject to regulations pursuant to the xx Act, I would like to confirm if it is possible to conduct xx in my new business activities without obtaining a permit pursuant to the xx Act.” instead of, for example, “Are the xx regulations an obstacle?”

**(3) Response**

- (i) The section to which the inquiry form was forwarded shall, in the case where the Strategy Development Division, the Strategy Development and Management Bureau has decided to respond, issue a written response to the submitter by using Form 6 of the Ordinance for Enforcement of the Enhancement Act within one month, in principle, from when the inquiry form or copy thereof arrived from the submitter at the contact point for inquiry. The section to which the inquiry form was forwarded shall, if there are unavoidable circumstances that prevent the issuance of a written response within the above period, in light of the status of examination of the interpretation of the provisions of the laws and ordinances and the presence or absence of application related to the request for confirmation stated in the inquiry form, notify the fact and its reason to the submitter every period that is no longer than one

month, until said written response is issued.

- (ii) In the case where the Commissioner of the FSA received the request from the head of another relevant administrative organ pursuant to provisions of Article 9(3) of the Enhancement Act, the section to which the inquiry form was forwarded shall, based on Article 9(1), state in the written response using Form 6 of the Ordinance for Enforcement of the Enhancement Act the interpretation and presence or absence of application of the provisions of the laws and ordinances related to said request within one month, in principle, from the day when the minister in charge set forth in Article 9(1) received submission of the inquiry form and copy thereof, pursuant to the same paragraph, and send it to said minister in charge through the Strategy Development Division, the Strategy Development and Management Bureau.

In such case, if there are unavoidable circumstances that prevent the issuance of a written response within the above period, in light of the status of examination of the interpretation of the provisions of the laws and ordinances and the presence or absence of application related to said request, notify the fact and its reason to said minister in charge through the Strategy Development Division, the Strategy Development and Management Bureau every period that is no longer than one month, until said written response is issued.

- (iii) In the case where the Commissioner of the FSA requested confirmation from the head of another relevant administrative organ pursuant to Article 9(3) of the Enhancement Act, when the Commissioner was sent a written response using Form 6 of the Ordinance for Enforcement of the Enhancement Act from said head of another relevant administrative organ, said written response shall be issued to the submitter through the Strategy Development Division, the Strategy Development and Management Bureau or the section to which an inquiry form was forwarded regarding the same matter as said request of confirmation. In addition, in the case where notification was received from said head of another relevant administrative organ to the effect that a written response cannot be issued within one month, in principle, as well as the reason, shall be notified to the submitter.

## **II-3 Points to Consider when Providing Administrative Guidance, etc.**

### **II-3-1 Points to Consider when Providing Administrative Guidance, etc.**

When providing administrative guidance, etc. (“Administrative guidance, etc.” includes administrative guidance as specified under Article 2(vi) of the Administrative Procedure Act as well as the advice and other acts that cannot be clearly distinguished from administrative guidance) to financial market infrastructures, supervisory departments shall abide by the Administrative Procedure Act and other relevant laws and regulations. The following points shall be taken into consideration.

#### **(1) General Principles (Article 32 of the Administrative Procedure Act)**

- (i) Whether the administrative guidance is followed entirely on the basis of voluntary cooperation of the supervised financial market infrastructures. For example, the following points shall be taken into consideration:
  - A. Whether the supervisor has obtained the understanding of the supervised financial market infrastructures on the contents and application of the administrative guidance, and the conduct of the official in charge.
  - B. Whether the administrative guidance has been continued despite the expression of an unwillingness to cooperate by the financial market infrastructures.
- (ii) Whether the supervisor has given unfavorable treatment to a financial market infrastructure for failing to follow administrative guidance.
  - A. It should be kept in mind that disclosing a failure to follow administrative guidance without due legal grounds could amount to “unfavorable treatment” in a situation where such disclosure would serve as a social punishment by causing economic losses, for example.
  - B. In cases where the authority to take administrative actions may be exercised depending on the circumstances following the provision of administrative guidance, the supervisor may provide the administrative guidance, while indicating the possibility of the exercise of the said authority.

#### **(2) Administrative Guidance Related to Applications (Article 33 of the Administrative Procedure Act)**

Whether the supervisor has prevented the applicant’s exercise of its rights by continuing administrative guidance, despite the applicant’s expression of an intention not to follow the said administrative guidance.



- (i) Even if the applicant has not clearly expressed an intention not to follow administrative guidance, the supervisory departments shall consider whether the applicant has no intention to do so by taking into consideration the background to the administrative guidance and changes in the objective circumstances, etc.
- (ii) It should be kept in mind that even if the applicant is following administrative guidance, this does not necessarily constitute voluntary consent to the supervisor's possible suspension of the screening and response processes regarding the application.
- (iii) The following points shall be taken into consideration, for example:
  - A. Whether the supervisor has prevented the applicant's exercise of its rights by putting the applicant in a situation in which it is impossible not to follow administrative guidance.
  - B. In cases where the applicant has not clearly expressed an intention to not follow administrative guidance, whether the supervisor has not suspended the screening and response processes regarding the application on the grounds that the applicant is receiving administrative guidance
  - C. In cases where the applicant has expressed an intention to not follow administrative guidance, whether the supervisor has ceased the said administrative guidance, and processed the application in a prompt and appropriate manner.

**(3) Administrative Guidance Concerning Authority over Granting of License and Approval (Article 34 of the Administrative Procedure Act)**

In cases where the supervisor does not have the authority to grant a license or approval or take administrative actions based thereon, or where the supervisor has no intention to exercise such authority, whether the supervisor is forcing a financial market infrastructure to follow administrative guidance by making an ostensible show of the possibility of exercising the authority.

For example, the following points shall be taken into consideration:

- (i) Whether the supervisor is requiring a financial market infrastructure to engage in or refrain from engaging in a particular act by pretending to have the authority to deny a license or approval in cases where the supervisor does not in reality have such authority.
- (ii) Whether the supervisor is forcing a financial market infrastructure to follow administrative guidance by indicating the possibility of exercising the authority regarding licensing and approval at any time unless the administrative guidance is followed, or by implying that some kind of unfavorable treatment would be given.

**(4) Method of Administrative Guidance (Article 35 of the Administrative Procedure Act)**

- (i) When providing administrative guidance, whether the supervisor makes it clear to the supervised financial market infrastructures what the purpose and contents of the said guidance, etc. are and who the officer in charge is.

The following points shall be taken into consideration, for example:

- A. Whether the supervisor clarifies what act the supervised financial market infrastructures should engage in or refrain from engaging in.
  - B. Whether the supervisor indicates which officer is responsible for the provision of relevant administrative guidance.
  - C. In cases where administrative guidance is provided based on a specific law, whether the supervisor indicates the legal provision used as the basis.
  - D. In cases where the provided administrative guidance is not based on a specific law, whether the supervisor gains the understanding of the financial market infrastructures of the necessity of the said guidance by explaining the purpose thereof.
- (ii) In cases where the supervised financial market infrastructure requests the provision of a document that specifies the officer in charge and the purpose and contents of administrative guidance, whether the supervisor meets the request in principle, unless there is any particular problem from the viewpoint of the conduct of administration (excluding cases that fit the description of either item of Article 35 (3)).

The following points shall be taken into consideration, for example:

- A. In cases where the provision of a written document is requested, it is necessary to meet the request as soon as possible.
- B. A “particular problem from the viewpoint of the conduct of administration” that justifies a refusal to provide the requested document refers to the case in which a significant impediment could be caused to the conduct of administration by the indication in writing of the officer in charge and the purpose and contents of administrative guidance. For example, if the document specifying those matters is utilized or interpreted regardless of the intention of the person who compiled it, achieving a certain administrative objective could become impossible.
- C. It should be kept in mind that a large backlog of work to be conducted or a need to conduct work in a short period of time alone would not constitute a “particular problem from the viewpoint of the conduct of administration.”

### **II-3-2 Points to Consider when Holding Interviews, etc.**

When FSA employees hold interviews, etc. (“interviews, etc.” include face-to-face interviews, telephone conversations and e-mail exchanges; the same shall apply hereinafter) with officers

and employees of financial market infrastructures, they shall take the following points into consideration:

- (1) Whether the FSA employees who participate in interviews, etc. always maintain discipline and decorum as well as a calm and composed attitude.
- (2) Whether FSA employees confirm the purpose of interviews, etc., and the names and affiliation of the interviewees.
- (3) Whether FSA employees ensure that the place and time of their interviews, etc., as well as the composition of participants from the FSA side and the interviewed financial market infrastructures are appropriate in light of the purpose and contents thereof.
- (4) Whether FSA officials make sure, as necessary, to have both sides share the recognition of the contents and results of interviews, etc. In particular, when the contents and results of an interview, etc. are subject to a confidentiality obligation, whether it is ensured that the need for confidentiality is made clear to both sides.
- (5) In cases where FSA officials face a need to consult their superiors with regard to the contents of interviews, etc., whether they seek the superiors' judgment in advance or make a report to the superiors immediately after the interviews, etc., depending on the circumstances. Furthermore, when they hold interviews with two or more financial market infrastructures regarding matters that require consultations with their superiors, whether FSA officials take care to ensure the consistency and transparency of the conduct of administration.

## **II-4 Points to Consider when Taking Administrative Actions**

### **II-4-1 Clearing Organizations**

#### **II-4-1-1 Response to Inspection Results, etc.**

##### **(1) Response to Inspection Results**

Supervisory departments shall properly reflect the results of inspections of COs conducted by inspection departments in supervisory processes as follows:

(i) Regarding violations of laws pointed out in inspection reports, and acts and situations that are related to the business operations and assets of the CO, and that are problematic from the viewpoint of protecting public interests and investors, as well as important matters pointed out in the previous inspection regarding which improvement is not sufficient, supervisory departments shall order, under Article 156-15 of the FIEA, the submission within one month (the deadline for the submission may be shortened on an item-by-item basis) of a report on factual confirmation, the analysis of causes, improvement and corrective measures, and other particulars, when they deem it necessary and appropriate to do so.

In addition, regarding a CO that is planning system modification, etc., and regarding which a problem has been pointed out with regard to the internal control environment for managing system modification risk, the supervisory departments shall order the submission of a report on the policy for implementing its plan for system modification, etc. precisely and on the internal control environment regarding the system risk (including internal audits), among other matters, when they deem it necessary and appropriate to do so.

(ii) When receiving the above reports, the supervisory departments shall hold sufficient hearings with the CO. When holding the hearings, the supervisory departments shall maintain close cooperation with inspection departments.

(iii) In cases where a certain period of time is deemed to be necessary in order to implement improvement and corrective measures specified in the reports and to make improvement regarding the matters pointed out in the inspection, the supervisory departments shall strive to ensure appropriate follow-up through periodic hearings, for example.

(iv) In cases where the SESC has issued a recommendation regarding administrative actions and other measures to be taken based on Article 20(1) of the Act for Establishment of the Financial Services Agency in consideration of onsite inspection

results, etc., supervisory authorities shall consider taking administrative actions based on Articles 156-15 to 156-17 of the FIEA and other appropriate measures after examining the contents of the recommendation.

**(2) Requirement for the Submission of Reports Based on Off-site Monitoring**

- (i) In cases where a CO is deemed to have a problem in its control environment for governance, risk management, compliance, etc. through off-site monitoring, etc., the supervisory departments shall require the submission of a report, based on Article 156-15 of the FIEA, on factual recognition regarding the problem, the analysis of the cause, improvement and corrective measures, and other necessary matters.
- (ii) In cases where it is deemed necessary to conduct more detailed investigation as a result of verifying the report, the supervisory departments shall require the submission of an additional report based on Article 156-15 of the FIEA.
- (iii) In cases where no serious problem from the viewpoint of protecting public interests and investors has been detected as a result of the examination of the above reports, and where it is deemed possible for the CO to make voluntary improvement efforts, the supervisory departments shall follow up on the reported improvement and corrective measures through in-depth hearings and other means.
- (iv) Furthermore, when necessary, the supervisory departments shall require the submission of periodic reports based on Article 156-15 of the FIEA and follow up thereon.

**II-4-1-2 Administrative Actions Based on Provisions of the FIEA (Business Improvement Orders, Business Suspension Orders, etc.)**

In cases where a serious problem from the viewpoint of protecting public interests and investors has been detected as a result of the examination of the contents of reports submitted by COs, or the contents of recommendations issued by inspection departments in light of the viewpoints specified in these Guidelines, the supervisory departments shall decide which administrative actions to take with due consideration of the factors described in (1) to (3) below after considering, among other factors, the following points:

- Whether it is appropriate to leave it to the CO to make improvement efforts on a voluntary basis.
- Whether substantial improvement is required and it is necessary to have the CO concentrate on business improvement for a certain period of time.
- Whether it is appropriate to allow the CO to continue business operations.

## **(1) Seriousness and Maliciousness of Acts**

### **(i) Degree of Damage to Public Interests**

Whether the CO is undermining public interests significantly such as damaging confidence in the financial instruments markets by, for example, failing to perform key parts of the risk management procedures prescribed in business rules, etc.

### **(ii) Extent of Damage to Investors and Market Participants**

Whether the damage was incurred by a wide range of investors and market participants in large numbers. How serious the damage incurred by individual investors and market participants is.

### **(iii) Maliciousness of Acts**

Whether the CO has acted in a malicious way, such as by failing to take countermeasures on an ongoing basis despite having continually received many complaints from investors and market participants.

### **(iv) Duration and Repetitive Nature of Acts**

Whether the act in question committed by a CO has been committed for a long period of time. Whether the act has been committed repeatedly and continuously or only once. Whether the CO committed a similar illegal act in the past.

### **(v) Intentionality**

Whether the CO has committed the illegal/inappropriate act intentionally while recognizing the illegality and inappropriateness, or has done so through negligence.

### **(vi) Institutional Involvement**

Whether the act has been committed based on an individual employee's judgment or a manager has been involved. Also, whether any officers have been involved.

### **(vii) Presence or Absence of Cover-Up Actions**

Whether an attempt to cover up the act has been made after its illegality was recognized. Whether a cover-up, if one exists, was an institutional act.

### **(viii) Involvement of Anti-Social Forces**

Whether any anti-social forces have been involved. How much involvement, if any.

## **(2) Appropriateness of Control Environment for Governance and Business Operation**

(i) Whether the officers are fully aware of the importance of compliance and make sufficient efforts to ensure compliance.

(ii) Whether the internal audit section is adequately staffed and equipped to conduct audits and whether the division is functioning properly.

(iii) Whether the compliance and risk management divisions are adequately staffed and equipped to perform their tasks and whether they are functioning properly.

- (iv) Whether employees engaging in business are fully aware of the importance of compliance and whether sufficient internal training is provided.

### **(3) Attenuation Factors**

Whether there are attenuation factors, such as necessary action being taken voluntarily to rectify the situation before the administrative response.

### **II-4-1-3 Standard Processing Period**

In cases where administrative disposition referred to in II-4-1-2 above is to be issued, the supervisory departments shall implement the administrative disposition within one month from the receipt of letters of recommendations from inspection departments or reports if the submission of such reports is required (within two months in cases where the actions are based on laws that are under the joint jurisdiction of the FSA and other ministries and agencies).

(Note 1) In determining the timing of the “receipt of a report,” the following points shall be taken into consideration:

- A. In cases where the submission of a report based on the provision of laws is required twice or more (limited to cases where the submission of an additional report is required within the prescribed period from the receipt of the most recent report), the receipt of the last report shall be the starting point of the counting of the standard processing period.
- B. In cases where the submission of corrected or additional documents (excluding those concerning minor corrections and additions) is required, the receipt of the said documents shall be the starting point of the counting of the standard processing period.

(Note 2) The time necessary for legal explanations and hearings shall not be included in the counting of the standard processing period.

(Note 3) The standard processing period shall be applied on the basis of each item of information used as the basis for determining what supervisory action to take.

### **II-4-1-4 Removal of the Requirement for the Submission of Reports on Compliance with Business Improvement Orders**

In cases where business improvement orders are issued, the supervisory departments shall follow up on the COs’ business improvement efforts based on such orders and, in principle, require the submission of reports on the implementation of business improvement plans

submitted by the COs so as to promote such efforts. Regarding the follow-up and the requirement for the submission of reports, the following points shall be taken into consideration:

- (1) In cases where COs who have received business improvement orders are required to submit reports on the implementation of their business improvement plans for a specified period of time, the requirement shall be removed upon the arrival of the end of the said period.
- (2) In cases where COs who have received business improvement orders are required to submit reports on the implementation of their business improvement plans continuously without any set timeframe, the requirement shall be removed when it is recognized that sufficient improvement measures have been taken in line with their business improvement plans with regard to the problems that constituted the basis of the issuance of the orders. A decision on whether to remove the requirement shall be made in light of the implementation of improvement efforts as identified through the submitted reports and other means.

#### **II-4-1-5 Relation to the Administrative Procedure Act and Other Laws**

##### **(1) Relation to the Administrative Procedure Act**

It should be kept in mind that in cases where supervisory departments intend to take adverse dispositions that fall under Article 13(1)(i) of the Administrative Procedure Act, they must conduct hearings, and where they intend to take adverse dispositions that fall under item (ii) of that paragraph, they must grant an opportunity for explanation. (In cases where the provisions of the FIEA require that a hearing, etc. be held, an opportunity for hearing, etc. shall be granted pursuant to such provisions.)

It should also be kept in mind that, in both cases, when the supervisory departments take adverse dispositions, they must indicate the reason for the action (when they take adverse dispositions in writing, they must also indicate the reason for the action in writing) based on Article 14 of that Act.

In addition, it should be kept in mind that in cases where the supervisory departments take dispositions to refuse the grant of license/approval, etc. required in an application, they must indicate the reason for the action based on Article 8 of that Act (when they take dispositions to refuse the grant of license/approval, etc. in writing, they must also indicate the reason for the action in writing).

It should further be kept in mind that, in doing so, the supervisory departments are required to clarify the facts on which the disposition was based as well as the specific laws and regulations applied in taking the disposition, instead of simply indicating the basis



provisions alone.

**(2) Relation to the Administrative Appeals Act**

It should be kept in mind that in cases where supervisory departments take dispositions for which complaints may be filed, the relevant COs must be advised in writing that they are entitled to file complaints based on the provision of Article 82 of the Administrative Appeals Act.

**(3) Relation to the Administrative Case Litigation Act**

It should be kept in mind that in cases where supervisory departments take dispositions for which action for revocation of administrative disposition may be filed, the relevant COs must be advised in writing that they are entitled to file an action for revocation of administrative disposition based on Article 46 of the Administrative Case Litigation Act.

**II-4-1-6 System for Exchange of Opinions**

In cases where unfavorable dispositions are to be taken, it may be useful for supervisory departments to exchange opinions with the relevant COs at several levels upon their request, in addition to holding legal hearings and granting opportunities for making explanations based on the Administrative Procedure Act, in order to share the recognition of the facts that constitute the basis of the administrative actions and their seriousness.

In cases where a CO who has recognized the likelihood of becoming the target of an adverse disposition during the hearing process concerning the requirement for the submission of a report, etc. requests that an opportunity be provided for an exchange of opinions (refer to Note 1) between senior officials of the supervisory departments (refer to Note 2) and senior officials of the CO, and where the supervisory departments intend to take an adverse disposition that involves opportunities for hearings or explanations with respect to the CO, an opportunity for an exchange of opinions about the facts that constitute the basis of the adverse disposition and their seriousness, etc. shall be granted before the notification of the said opportunities for hearings and explanations, unless it is necessary to take the said administrative disposition urgently.

(Note 1) Requests from COs for an opportunity for an exchange of opinions shall be met only if they are made between the receipt of reports on the facts that constitute the basis of the relevant unfavorable dispositions that have been submitted based on the provisions of laws and the notification of opportunities for hearings and explanations by the supervisory authorities.

(Note 2) “Senior officials of the supervisory departments” include the directors-general of the

relevant divisions of the FSA.

#### **II-4-1-7 Notification to Relevant Authorities, including Foreign Supervisory Authorities**

In cases where supervisory departments intend to take unfavorable dispositions, including requiring the submission of reports, issuing orders for business improvement and business suspension and rescinding licenses, etc., they shall, as necessary, notify other relevant authorities in accordance with II-1-3.

#### **II-4-1-8 Concept on the Publication of Unfavorable Dispositions**

In cases where unfavorable dispositions have been taken, such as the rescission of licenses, etc., the facts that constitute the basis of unfavorable dispositions and the contents of the dispositions shall be published, in consideration of the highly public nature of the series of functions performed by COs, and in view of making administrative actions more predictable for other COs, etc. and thereby preventing similar incidents from occurring in the future, except for cases where the publication of those matters might cause significant market turmoil (if there are provisions on public notices, etc. in the FIEA, the procedures for public notices, etc. shall be performed pursuant to such provisions).

#### **II-4-1-9 Points for Attention Concerning Preparation of Documents Required to be Submitted by COs**

Regarding the statement of name of representatives in the Attached List of Formats, it should be kept in mind that persons who have stated their former surname (meaning the former surname prescribed in Article 30-13 of the Order for Enforcement of the Residential Basic Book Act (Cabinet Order No. 292 of 1967)) and given names together with their current name at the time of applying for a license, etc. may state their former surnames and given names in brackets next to their current name or state their former surnames and given names in place of their current name.

#### **II-4-1-10 Points of Attention Regarding Submitting Applications, etc. which can be filed electronically**

##### **(1) Points of Attention regarding procedures in paper or in person**

With respect to applications and notifications, etc. by the CO to the authorities, and notices of

disposition, etc. issued by the authorities to the CO, pursuant to the provisions of Article 6 (1) and Article 7(1) of the Act on the Promotion, etc. of Administration Utilizing Information and Communications Technology (hereinafter referred to as the "Digital Procedures Act"), respectively, notwithstanding the provisions of the relevant laws and regulations, such applications and notifications, etc. may be made by using an electronic data processing system, even if the provisions of the relevant laws and regulations prescribe that such applications and notifications, etc. shall be made in writing or by other means.

In light of the purpose of the Digital Procedures Act, the provisions of the Supervisory Guidelines pertaining to procedures subject to the Digital Procedures Act may also be conducted using an electronic data processing system, regardless of whether such procedures are prescribed to be conducted in writing or in person.

In addition, with the rapid progress of digitalization in all economic and social activities, the government as a whole is reviewing Japan's systems and practices that presuppose written documents, seals, and face-to-face procedures, and is working toward the realization of a remote society where procedures can be completed without actually visiting an office.

In order to steadily promote these efforts, the FSA has also been promoting the computerization of administrative procedures by revising The Electronic Application and Notification System of the FSA to enable online submission of all applications and notifications received from the CO, as well as revising the Cabinet Office Ordinance and Supervisory Guidelines to abolish the use of seals.

Furthermore, with regard to procedures among private businesses, the Government of Japan held the "Study Group for Reviewing Procedures in paper, in person and seals in the Financial Industry" to encourage the entire industry to review its practices, and has been working to digitize documents, eliminate the need for seals, and review face-to-face regulations.

Based on these efforts in the public and private sectors, excluding the cases where the original documents are required to be sent as described in (2), the application form can be submitted by using an electronic data processing system or other methods that utilize information communication technology.

In light of the purpose of the above-mentioned treatment, it is recommended that procedures based on the provisions of this Supervisory Guidelines be conducted, to the extent possible, in a manner other than in writing or in person, taking into consideration the intentions of the other party to the procedures.

## **(2) Points of Attention Regarding Submitting Applications, etc.**

Based on (1), applications and notifications, etc. by the CO to the authorities shall, in principle, be requested by the submission deadline stipulated by laws and regulations using the

Electronic Application and Notification System of the FSA.

However, for attached documents issued by public institutions (copy of resident certificate, ID card, copy of family register, documents certifying payment of taxes and fees, etc.), the original documents should be sent.

## **II-4-2 Fund Clearing Organizations**

### **II-4-2-1 Response to Inspection Results, etc.**

#### **(1) Response to Inspection Results**

Supervisory departments shall properly reflect the results of inspections of FCOs conducted by inspection departments in supervisory processes as follows:

(i) Regarding violation of laws pointed out in inspection reports, and acts and situations that are related to the business operations and assets of the FCO, and that are problematic from the viewpoint of conducting operations in an appropriate and reliable manner, as well as important matters pointed out in the previous inspection regarding which improvement is not sufficient, supervisory departments shall order, under Article 80 (1) of the PSA, the submission within one month (the deadline for the submission may be shortened on an item-by-item basis) of a report on factual confirmation, the analysis of causes, improvement and corrective measures and other particulars, when they deem it necessary to do so.

In addition, regarding an FCO that is planning system modification, etc., and regarding which a problem has been pointed out with regard to the internal control environment for managing system modification risk, the supervisory departments shall order the submission of a report on the policy for implementing its plan for system modification, etc. precisely and on the internal control environment regarding the system risk (including internal audits), among other matters, when they deem it necessary to do so.

(ii) When receiving the above reports, the supervisory departments shall hold sufficient hearings with the FCO. When holding the hearings, the supervisory departments shall maintain close cooperation with inspection departments.

(iii) In cases where a certain period of time is deemed to be necessary in order to implement improvement and corrective measures specified in the reports and to make improvement regarding the matters pointed out in the inspection, the supervisory departments shall strive to ensure appropriate follow-up through periodic hearings, for example.

## **(2) Requirement for the Submission of Reports Based on Off-site Monitoring**

- (i) In cases where an FCO is deemed to have a problem in its control environment for governance, risk management, compliance, etc. through off-site monitoring, etc., the supervisory departments shall require the submission of a report, based on Article 80(1) of the PSA on factual recognition regarding the problem, the analysis of the cause, improvement and corrective measures and other necessary matters.
- (ii) In cases where it is deemed necessary to conduct more detailed investigation as a result of verifying the report, the supervisory departments shall require the submission of an additional report based on Article 80(1) of the PSA.
- (iii) In cases where no serious problem from the viewpoint of conducting operations in an appropriate and reliable manner has been detected as a result of the examination of the above reports, and where it is deemed possible for the FCO to make voluntary improvement efforts, the supervisory departments shall follow up on the reported improvement and corrective measures through in-depth hearings and other means.
- (iv) Furthermore, when necessary, the supervisory departments shall require the submission of periodic reports based on Article 80(1) of the PSA and follow up thereon.

### **II-4-2-2 Administrative Actions Based on Provisions of the Payment Services Act (Business Improvement Orders, Business Suspension Orders, etc.)**

In cases where a serious problem from the viewpoint of conducting operations in an appropriate and reliable manner has been detected as a result of the examination of the contents of reports submitted by FCOs, or the contents of recommendations issued by inspection departments in light of the viewpoints specified in these Guidelines, the supervisory departments shall decide which administrative actions to take with due consideration of the factors described in (1) to (3) below after considering, among other factors, the following points:

- Whether it is appropriate to leave it to the FCO to make improvement efforts on a voluntary basis.
- Whether substantial improvement is required and it is necessary to have the FCO concentrate on business improvement for a certain period of time.
- Whether it is appropriate to allow the FCO to continue business operations.

#### **(1) Seriousness and Maliciousness of Acts**

##### **(i) Degree of Damage to Public Interests**

Whether the FCO is undermining the public interest significantly, such as by damaging confidence in the payment system by, for example, failing to perform key parts of the risk management procedures prescribed in business rules, etc.

**(ii) Extent of Damage to participants, etc.**

Whether the damage was incurred by a wide range of participants, etc. in large numbers. How serious the damage incurred by individual participants, etc. is.

**(iii) Maliciousness of Acts**

Whether the FCO has acted in a malicious way, such as by failing to take countermeasures on an ongoing basis despite having continually received many complaints from participants, etc.

**(iv) Duration and Repetitive Nature of Acts**

Whether the act in question committed by an FCO has been committed for a long period of time. Whether the act has been committed repeatedly and continuously or only once. Whether the FCO committed a similar illegal act in the past.

**(v) Intentionality**

Whether the FCO has committed the illegal/inappropriate act intentionally while recognizing the illegality and inappropriateness, or has done so through negligence.

**(vi) Institutional Involvement**

Whether the act has been committed based on an individual employee's judgment or a manager has been involved. Also, whether any officers have been involved.

**(vii) Presence or Absence of Cover-Up Actions**

Whether an attempt to cover up the act has been made after its illegality was recognized. Whether a cover-up, if one exists, was an institutional act.

**(viii) Involvement of Anti-Social Forces**

Whether any anti-social forces have been involved. How much involvement, if any.

**(2) Appropriateness of Control Environment for Governance and Business Operation**

- (i) Whether the officers are fully aware of the importance of compliance and make sufficient efforts to ensure compliance.
- (ii) Whether the internal audit section is adequately staffed and equipped to conduct audits and whether the division is functioning properly.
- (iii) Whether the compliance and risk management divisions are adequately staffed and equipped to perform their tasks and whether they are functioning properly.
- (iv) Whether employees engaging in business are fully aware of the importance of compliance and whether sufficient internal training is provided.

### **(3) Attenuation Factors**

Whether there are attenuation factors, such as necessary action being taken voluntarily to rectify the situation before the administrative response.

### **II-4-2-3 Standard Processing Period, etc.**

The provisions concerning COs that are prescribed in II-4-1-3 to II-4-1-10 shall be applied mutatis mutandis to the supervision of FCOs. When those provisions are thus applied mutatis mutandis, “letters of recommendations from inspection departments or reports if the submission of such reports is required” shall be replaced with “reports if the submission of such reports is required.”

### **II-4-3 Book-entry Transfer Institutions**

#### **II-4-3-1 Response to Inspection Results, etc.**

##### **(1) Response to Inspection Results**

Supervisory departments shall properly reflect the results of inspections of BeTIs conducted by inspection departments in supervisory processes as follows:

- (i) Regarding the violation of laws pointed out in inspection reports, and acts and situations that are related to the business operations and assets of the BeTIs, and that are problematic from the viewpoint of conducting operations in an appropriate and reliable manner, as well as important matters pointed out in the previous inspection regarding which improvement is not sufficient, supervisory departments shall order, under Article 20(1) of the Book-Entry Transfer Act, the submission within one month (the deadline for the submission may be shortened on an item-by-item basis) of a report on factual confirmation, the analysis of causes, improvement and corrective measures, and other particulars, when they deem it necessary to do so.

In addition, regarding a BeTI that is planning system modification, etc., and regarding which a problem has been pointed out with regard to the internal control environment for managing system modification risk, the supervisory departments shall order the submission of a report on the policy for implementing its plan for system modification, etc. precisely and on the internal control environment regarding the system risk (including internal audits), among other matters, when they deem it necessary to do so.

- (ii) When receiving the above reports, the supervisory departments shall hold sufficient hearings with the BeTIs. When holding the hearings, the supervisory departments shall

maintain close cooperation with inspection departments.

- (iii) In cases where a certain period of time is deemed to be necessary in order to implement improvement and corrective measures specified in the reports and to make improvement regarding the matters pointed out in the inspection, the supervisory departments shall strive to ensure appropriate follow-up through periodic hearings, for example.
- (iv) In cases where the SESC issues a recommendation regarding administrative actions and other measures to be taken based on Article 20(1) of the Act for Establishment of the Financial Services Agency in consideration of onsite inspection results, etc., supervisory authorities shall consider taking administrative actions based on Articles 20 to 23 of the Book-Entry Transfer Act and other appropriate measures after examining the contents of the recommendation.

## **(2) Requirement for the Submission of Reports Based on Off-site Monitoring**

- (i) In cases where a BeTI is deemed to have a problem in its control environment for governance, risk management, compliance, etc. through off-site monitoring, etc., the supervisory departments shall require the submission of a report, based on Article 20(1) of the Book-Entry Transfer Act, on factual recognition regarding the problem, the analysis of the cause, improvement and corrective measures, and other necessary matters.
- (ii) In cases where it is deemed necessary to conduct more detailed investigation as a result of verifying the report, the supervisory departments shall require the submission of an additional report based on Article 20(1) of the Book-Entry Transfer Act
- (iii) In cases where no serious problem from the viewpoint of conducting book-entry transfer operations in an appropriate and reliable manner and protecting investors has been detected as a result of the examination of the above reports, and where it is deemed possible for the BeTIs to make voluntary improvement efforts, the supervisory departments shall follow up on the reported improvement and corrective measures through in-depth hearings and other means.
- (iv) Furthermore, when necessary, the supervisory departments shall require the submission of periodic reports based on Article 20(1) of the Book-Entry Transfer Act and follow up thereon.

### **II-4-3-2 Administrative Actions Based on Provisions of the Book-Entry Transfer Act (Business Improvement Orders, Business Suspension Orders, etc.)**



In cases where a serious problem from the viewpoint of conducting book-entry transfer operations in an appropriate and reliable manner has been detected as a result of the examination of the contents of reports submitted by BeTIs, or the contents of recommendations issued by inspection departments in light of the viewpoints specified in these Guidelines, the supervisory departments shall decide which administrative actions to take with due consideration of the factors described in (1) to (3) below after considering, among other factors, the following points:

- Whether it is appropriate to leave it to the BeTI to make improvement efforts on a voluntary basis.
- Whether substantial improvement is required and it is necessary to have the BeTI concentrate on business improvement for a certain period of time.
- Whether it is appropriate to allow the BeTI to continue business operations.

**(1) Seriousness and Maliciousness of Acts**

**(i) Degree of Damage to Public Interests**

Whether the BeTI is undermining the public interests significantly such as by damaging confidence in the financial instruments markets by, for example, failing to perform key parts of the procedures prescribed in Business rules, etc.

**(ii) Extent of Damage to Investors and Market Participants**

Whether the damage was incurred by a wide range of investors and market participants in large numbers. How serious the damage incurred by individual investors and market participants is.

**(iii) Maliciousness of Act**

Whether the BeTIs have acted in a malicious way, such as by failing to take countermeasures on an ongoing basis despite having continually received many complaints from investors and market participants.

**(iv) Duration and Repetitive Nature of Acts**

Whether the act in question committed by a BeTI has been committed for a long period of time. Whether the act has been committed repeatedly and continuously or only once. Whether the BeTI committed a similar illegal act in the past.

**(v) Intentionality**

Whether the BeTI has committed the illegal/inappropriate act intentionally while recognizing the illegality and inappropriateness, or has done so through negligence.

**(vi) Institutional Involvement**

Whether the act has been committed based on an individual employee's judgment or a manager has been involved. Also, whether any officers have been involved.

**(vii) Presence or Absence of Cover-Up Actions**

Whether an attempt to cover up the act has been made after its illegality was recognized. Whether a cover-up, if one exists, was an institutional act.

**(viii) Involvement of Anti-Social Forces**

Whether any anti-social forces are involved. How much involvement, if any.

**(2) Appropriateness of Control Environment for Governance and Business Operation**

- (i) Whether the officers are fully aware of the importance of compliance and make sufficient efforts to ensure compliance.
- (ii) Whether the internal audit section is adequately staffed and equipped to conduct audits and whether the division is functioning properly.
- (iii) Whether the compliance and risk management divisions are adequately staffed and equipped to perform their tasks and whether they are functioning properly.
- (iv) Whether employees engaging in business are fully aware of the importance of compliance and whether sufficient internal training is provided.

**(3) Attenuation Factors**

Whether there are attenuation factors, such as necessary action being taken voluntarily to rectify the situation before the administrative response.

**II-4-3-3 Standard Processing Period, etc.**

The provisions concerning COs that are prescribed in II-4-1-3 to II-4-1-10 shall be applied mutatis mutandis to the supervision of BeTIs.

**II-4-4 Trade Repositories**

**II-4-4-1 Response to Inspection Results, etc.**

**(1) Response to Inspection Results**

Supervisory departments shall properly reflect the results of inspections of TRs and entities to which part of the trade repositories operations are outsourced (hereinafter referred to as “TRs, etc.”) conducted by inspection departments in supervisory processes as follows:

- (i) Regarding violation of laws pointed out in inspection reports, and acts and situations that are related to the business operations and assets of the TR, and that are problematic

from the viewpoint of protecting public interests and investors, as well as important matters pointed out in the previous inspection regarding which improvement is not sufficient, supervisory departments shall order, under Article 156-80 of the FIEA, the submission within one month (the deadline for the submission may be shortened on an item-by-item basis) of a report on factual confirmation, the analysis of causes, improvement and corrective measures and other particulars, when they deem it necessary and appropriate to do so.

In addition, regarding a TR, etc. that is planning system modification, etc., and regarding which a problem has been pointed out with regard to the internal control environment for managing system modification risk, the supervisory departments shall order the submission of a report on the policy for implementing its plan for system modification, etc. precisely and on the internal control environment regarding the system risk (including internal audits), among other matters, when they deem it necessary and appropriate to do so.

- (ii) When receiving the above reports, the supervisory departments shall hold sufficient hearings with the TR, etc. When holding the hearings, the supervisory departments shall maintain close cooperation with inspection departments.
- (iii) In cases where a certain period of time is deemed to be necessary in order to implement improvement and corrective measures specified in the reports and to make improvement regarding the matters pointed out in the inspection, the supervisory departments shall strive to ensure appropriate follow-up through periodic hearings, for example.
- (iv) In cases where the SESC has issued a recommendation regarding administrative actions and other measures to be taken based on Article 20(1) of the Act for Establishment of the Financial Services Agency in consideration of onsite inspection results, etc., supervisory authorities shall consider taking administrative actions based on Articles 156-80, 81, 83 and 84 of the FIEA, and other appropriate measures after examining the contents of the recommendation.

## **(2) Requirement for the Submission of Reports Based on Off-site Monitoring**

- (i) In cases where a TR is deemed to have a problem in its control environment for governance, risk management, compliance, etc. through off-site monitoring, etc., the supervisory departments shall require the submission of a report, based on Article 156-80 of the FIEA, on factual recognition regarding the problem, the analysis of the cause, improvement and corrective measures, and other necessary matters.
- (ii) In cases where it is deemed necessary to conduct more detailed investigation as a result

of verifying the report, the supervisory departments shall require the submission of an additional report based on Article 156-80 of the FIEA.

(iii) In cases where no serious problem from the viewpoint of protecting the public interest and investors has been detected as a result of the examination of the above reports, and where it is deemed possible for the TR to make voluntary improvement efforts, the supervisory departments shall follow up on the reported improvement and corrective measures through in-depth hearings and other means.

(iv) Furthermore, when necessary, the supervisory departments shall require the submission of periodic reports based on Article 156-80 of the FIEA and follow up thereon.

#### **II-4-4-2 Administrative Actions Based on Provisions of the FIEA (Business Improvement Orders, Business Suspension Orders, etc.)**

In cases where a serious problem from the viewpoint of protecting the public interest and investors has been detected as a result of the examination of the contents of reports submitted by TRs, etc., or the contents of recommendations issued by inspection departments in light of the viewpoints specified in these Guidelines, the supervisory departments shall decide which administrative actions to take with due consideration of the factors described in (1) to (3) below after considering, among other factors, the following points:

- Whether it is appropriate to leave it to the TR to make improvement efforts on a voluntary basis.
- Whether substantial improvement is required and it is necessary to have the TR concentrate on business improvement for a certain period of time.
- Whether it is appropriate to allow the TR to continue business operations.

#### **(1) Seriousness and Maliciousness of Acts**

##### **(i) Degree of Damage to Public Interests**

Whether the TR is undermining the public interests significantly, such as by damaging confidence in the financial instruments markets by, for example, failing to perform key parts of the procedures prescribed in Business rules, etc.

##### **(ii) Extent of Damage to Investors and Market Participants**

Whether the damage was incurred by a wide range of investors and market participants in large numbers. How serious the damage incurred by individual investors and market participants is.

##### **(iii) Maliciousness of Acts**

Whether the TR has acted in a malicious way, such as by failing to take

countermeasures on an ongoing basis despite having continually received many complaints from investors and market participants.

**(iv) Duration and Repetitive Nature of Acts**

Whether the act in question committed by a TR has been committed for a long period of time. Whether the act has been committed repeatedly and continuously or only once. Whether the TR committed a similar illegal act in the past.

**(v) Intentionality**

Whether the TR has committed the illegal/inappropriate act intentionally while recognizing the illegality and inappropriateness, or has done so through negligence.

**(vi) Institutional Involvement**

Whether the act has been committed based on an individual employee's judgment or a manager has been involved. Also, whether any officers have been involved.

**(vii) Presence or Absence of Cover-Up Actions**

Whether an attempt to cover up the act has been made after its illegality was recognized. Whether a cover-up, if one exists, was an institutional act.

**(viii) Involvement of Anti-Social Forces**

Whether any anti-social forces have been involved. How much involvement, if any.

**(2) Appropriateness of Control Environment for Governance and Business Operation**

- (i) Whether the officers are fully aware of the importance of compliance and make sufficient efforts to ensure compliance.
- (ii) Whether the internal audit section is adequately staffed and equipped to conduct audits and whether the division is functioning properly.
- (iii) Whether the compliance and risk management divisions are adequately staffed and equipped to perform their tasks and whether they are functioning properly.
- (iv) Whether employees engaging in business are fully aware of the importance of compliance and whether sufficient internal training is provided.

**(3) Attenuation Factors**

Whether there are attenuation factors, such as necessary action being taken voluntarily to rectify the situation before the administrative response.

**II-4-4-3 Standard Processing Period, etc.**

The provisions concerning COs that are prescribed in II-4-1-3 to II-4-1-10 shall be applied mutatis mutandis to the supervision of TRs.

### **III. Supervisory Viewpoints and Procedures (Clearing Organizations)**

#### **III-1 Governance / Business Administration**

##### **III-1-1 Governance System**

###### **(1) Background and Objectives**

More appropriate risk management, etc. than ever is required for COs as their operations are becoming increasingly complex. Under these circumstances, there shall be effective disciplines for management and proper governance in COs, in order to ensure appropriate business operations and sound management of COs, and in turn, financial system stability.

Effective functioning of governance presumes that the components of the organization are fulfilling their primary roles. Specifically, it is important that, for example, organs such as the board of directors and the board of auditors are able to check management, and checks and balances among divisions are functioning properly, as is the internal audit section. It is also necessary for representative directors, directors, executive officers, auditors and employees in all positions to understand their respective roles and be fully involved in the process.

(Note) In the case of COs that have established nominating committees, etc., it is necessary to examine whether the board of directors, nominating committees, executive officers, etc. are properly exercising their respective authority. In addition, in the case of COs that have established an audit and supervisory committee, it is necessary to examine whether the board of directors and audit and supervisory committee, etc. are properly exercising their respective authority. In this case, examination should be conducted with due consideration of the actual status of management based on the purpose of these Guidelines.

###### **(2) Major Supervisory Viewpoints**

###### **[Representative Director]**

- (i) Whether the representative director considers compliance as one of the important management issues and takes the initiative in building a control environment for compliance.
- (ii) Whether the representative director fully recognizes that disregarding the risk management division may have a serious impact on corporate earnings and attaches importance to the said division.

### **[Directors/Board of Directors]**

- (i) Whether directors check and prevent autocratic management by the representative director and other officers who are responsible for business execution, and are actively involved in the board of directors' decision-making and checking process concerning business execution.
- (ii) In cases where outside directors are appointed, whether they recognize their own significance from the viewpoint of ensuring objectivity in the decision-making of management, etc. and proactively participate in the meetings of the board of directors. In cases where proposals for the appointment of outside directors are to be determined, whether the outside directors' personal relationships and equity relationships with the CO and other interests are verified and their independence, aptitude, etc. are carefully examined, in consideration of the roles they are expected to fulfill. Whether some kind of framework has been established so that outside directors would make appropriate judgments at the meetings of the board of directors; for example, whether information is provided on an ongoing basis.
- (iii) Whether the board of directors takes measures to objectively ensure the appropriateness and fairness of, for example, important management decisions and management judgments related to compliance, credit risk management, etc. such as utilizing the advice of outside experts and discretionary committees whose members consist of outside experts as necessary when making such decisions and judgments. In particular, whether the board of directors takes measures to appropriately reflect the legitimate interests of its direct and indirect participants and other relevant stakeholders on design, rules, overall strategy, and major decisions.
- (iv) Whether the board of directors has specified a management policy based on the overall vision of the desirable status of the CO. Whether it has established management plans in line with the management policy and communicated the plans throughout the organization. Whether it regularly reviews and revises the progress status thereof.
- (v) Whether directors and the board of directors are sincerely leading efforts in compliance and are properly demonstrating the board's functions to establish an organization-wide internal control environment.
- (vi) Whether the board of directors fully recognizes that disregarding the risk management division may have a serious impact on corporate earnings, and attaches importance to the said division. In particular, whether the director in charge has in-depth knowledge and understanding concerning the methods of measuring, monitoring and managing risks, in addition to an understanding of where risks reside and what kind of risks they are.
- (vii) Whether the board of directors has set up a policy for managing risks based on

strategic objectives and communicated it throughout the organization. Whether it reviews the risk management policy on a periodic or as-needed basis. In addition, whether the board of directors makes use of risk-related information in the execution of business and the development of risk management systems by, for example, making necessary decisions based on the status of risks reported periodically.

**[Auditors/Board of Auditors]**

- (i) Whether the independence of the auditors and the board of auditors is ensured in accordance with the purpose of the board of auditors system.
- (ii) Whether the auditors and the board of auditors properly exercise the broad authority granted thereto and conduct audits of business operations in addition to audits of accounting affairs.
- (iii) Whether individual auditors recognize the importance of their own independence within the board of auditors and actively take the initiative to conduct audits.
- (iv) Whether the auditors and the board of auditors strive to ensure the effectiveness of their audits by, for example, receiving reports on the results of external audits, depending on the contents thereof.

**[Internal Audit Section]**

- (i) Whether the internal audit section is independent from divisions subject to audit so as to fully check the actions thereof, has the control environment and ability to collect important information on their operational status, etc. in a timely manner, and is sufficiently staffed and equipped to conduct effective internal audits that are accurately adapted to the environment surrounding the CO and its operational status.
- (ii) Whether the internal audit section formulates efficient and effective internal audit plans that give consideration to frequency and depth according to the type and magnitude of risks based on its understanding of the status of risk management, etc. by divisions subject to audits, properly reviews the plans depending on the situation, and conducts efficient and effective internal audits based on the internal audit plans.
- (iii) Whether the internal audit section reports important issues pointed out in internal audits without any delay to the representative director and the board of directors. Whether the internal audit section has accurately identified the status of improvements made on the issues pointed out.

**[Use of External Audits]**

- (i) Whether external audits are effectively utilized, with sufficient understanding that



effective external audits are indispensable for ensuring sound and appropriate business operations of COs.

- (ii) Whether external audits are examined periodically as to whether they are effectively functioning, and appropriate measures are taken with respect to the external audit results, etc.
- (iii) Whether such matters as the number of consecutive years of service by a certified public accountant involved are handled properly.

### **(3) Supervisory Method and Actions**

Supervisory departments shall examine the status of governance through the following hearings and daily supervisory administrative processes.

#### **(i) Comprehensive Hearings (See II-1-1 (1))**

Supervisory departments shall hold hearings regarding COs' management challenges, strategies and the status of risk management and governance, among other matters. In addition, senior supervisory departments shall directly hold hearings with top managers of COs as necessary.

#### **(ii) Examination of Governance through Daily Supervisory Administrative Processes**

Supervisory departments shall examine the effectiveness of governance not only through the hearings described above but also through daily supervisory administrative processes, such as follow-up on reports on business improvements made on matters pointed out in inspections.

#### **(iii) Recording of Monitoring Results**

Supervisory departments shall compile and store records on matters of particular note based on the results of monitoring conducted through procedures described above, and make effective use thereof in future supervisory administrative processes.

#### **(iv) Supervisory Method and Actions**

In cases where doubt has arisen about the effectiveness of a CO's governance, the supervisory departments shall monitor voluntary business improvement made by the CO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-15 of the FIEA.

Furthermore, the supervisory departments shall take actions such as issuing an order for business improvement based on Article 156-16 of the FIEA, when it is deemed necessary and appropriate to do so from the viewpoint of protecting public interests and investors.

### **III-1-2 Officers of Clearing Organizations**

#### **(1) Major Supervisory Viewpoints**

From the viewpoint of maintaining the public nature of financial instruments obligation assumption service, supervisory departments shall pay attention to the following points when examining the decision-making process regarding proposals for the appointment of officers of the CO, among others.

- (i) The officer shall neither meet any of the ineligibility criteria (Article 82(2)(iii)(a) to (f) of the FIEA) nor have met any of them at the time when the CO obtained a license or approval.
- (ii) The officer shall neither have violated laws and regulations regarding financial instruments obligation assumption service or business incidental thereto nor have breached any administrative actions taken based on laws and regulations.
- (iii) The officer shall not have engaged in an illegal or markedly inappropriate act regarding financial instruments obligation assumption service under particularly grave circumstances.

#### **(2) Supervisory Method and Actions**

Supervisory departments shall consider taking actions such as ordering the dismissal of an officer of a CO under the provision of Article 156-14(3) or Article 156-17(2) of the FIEA when said officer: (i) meets any criteria specified in Article 82(2)(iii)(a) to (f) of the FIEA, or is found to have already met such criteria at the time when the CO obtained license or approval; (ii) is found to have become an officer of the CO by fraudulent means; or (iii) violates or is found to have violated laws and regulations or administrative actions taken based on laws and regulations.

In addition, they shall hold an in-depth hearing regarding the decision-making process concerning the proposal for the appointment of the said officer or committee member and, when necessary, require the submission of a report based on Article 156-15 of the FIEA. Furthermore, supervisory departments shall consider taking actions, such as issuing an order for business improvement (Article 156-16 of the FIEA), if the CO's control environment for governance is deemed to have a serious problem and the action is deemed to be necessary and appropriate, from the viewpoint of protecting public interests and investors.

### **III-1-3 Staffing**

## **(1) Major Supervisory Viewpoints**

Supervisory departments shall examine whether COs are adequately staffed to properly and reliably conduct financial instruments obligation assumption service, in light of the following requirements regarding COs' officers and employees.

- (i) Whether the COs have secured officers and employees who understand the viewpoints regarding governance that are specified under the FIEA and other relevant regulations, as well as these Guidelines, and who have the knowledge and experience necessary for conducting governance as well as sufficient knowledge and experience concerning the control environment for compliance and risk management required to properly and reliably execute the financial instruments obligation assumption service.
- (ii) Whether officers or employees are current or former members of organized crime groups (meaning organized crime group members prescribed in Article 2(vi) of the Act on Prevention of Unjust Acts by Organized Crime Group Members; the same shall apply hereinafter) or have a close relationship with organized crime groups (meaning organized crime groups prescribed in Article 2(ii) of the Act on Prevention of Unjust Acts by Organized Crime Group Members; the same shall apply hereinafter).
- (iii) Whether officers or employees have the experience of being sentenced to a fine (including similar punishments imposed under foreign laws and regulations equivalent thereto) for violation of the FIEA or other domestic financial laws and regulations or foreign laws and regulations equivalent thereto.
- (iv) Whether officers or employees have the experience of being sentenced to a fine (including similar punishments imposed under foreign laws and regulations equivalent thereto) for violation of the Act on Prevention of Unjust Acts by Organized Crime Group Members (excluding the provisions of Article 32-3(7) and Article 32-11(1) of said Act) or other foreign laws and regulations equivalent thereto, or for committing a crime prescribed under the Penal Code or under the Act on Punishment of Physical Violence and Others.
- (v) Whether officers or employees have the experience of being sentenced to imprisonment with work or more severe punishment (including similar punishments imposed under foreign laws or regulations equivalent thereto). In particular, whether officers or employees have been accused of committing crimes specified under Articles 246 to 250 of the Penal Code (fraud, fraud using computers, breach of trust, quasi fraud and extortion as well as attempts at these crimes).

## **(2) Supervisory Method and Actions**

The requirements specified in (i) to (v) above are part of a comprehensive set of

elements that should be taken into consideration when supervisory departments examine whether a CO is adequately staffed to properly and reliably conduct financial instruments obligation assumption service. Even if an officer or an employee is deemed to not meet the requirements, it should not automatically lead to the conclusion that the CO is not adequately staffed. The important thing is, first and foremost, that COs strive to ensure on their own responsibility that they are adequately staffed, in light of those requirements and other elements.

However, supervisory departments shall hold in-depth hearings regarding the CO's awareness of such staffing and the decision-making process concerning the proposed appointments of officers and employees, in cases where a CO is deemed to have failed to take those elements into consideration sufficiently in the said decision-making process, and where it is deemed to be necessary and appropriate to hold such hearings in relation to the business operations of the CO from the viewpoint of protecting public interests and investors. In addition, they shall require the submission of reports under the provision of Article 156-15 of the FIEA when necessary.

Supervisory departments shall consider taking actions such as issuing an order for business improvement under Article 156-16 of the FIEA, in cases where the CO's control environment for governance is deemed to have a serious problem as a result of the examination of the submitted report, and where the action is deemed to be necessary and appropriate from the viewpoint of protecting public interests and investors.

## **III-2 Financial Soundness**

### **III-2-1 Adequacy of Capital**

#### **(1) Background and Objectives**

In order for COs to gain participants' and market players' confidence and to operate their business continuously and stably, it is important for COs to retain a sufficient financial basis according to the characteristics of management as well as to establish appropriate arrangements and procedures for managing credit risks, liquidity risks and other such risks.

Accordingly, COs should hold enough liquid assets to withstand any losses that may be incurred in the event that various risks are actualized.

COs also need to have a process for evaluating their capital adequacy in the context of their risk profiles, and implement appropriate measures for maintaining a sufficient level of capital.

#### **(2) Major Supervisory Viewpoints**

##### **[Directors/Board of Directors]**

- (i) Whether the directors have a general understanding of the nature and level of the risks taken by the CO as well as the relationship between risk and the appropriate level of capital.
- (ii) Whether the directors and the board of directors understand that, in order to achieve their strategic objectives, a capital plan, which is consistent with them, is an essential component, and whether they have formulated an appropriate capital plan according to the management issues of the CO.
- (iii) Whether the directors have been sufficiently involved in formulating the aforementioned capital plan, and are adopting a process for evaluating capital adequacy and implementing appropriate measures for maintaining a sufficient level of capital.

##### **[Capital Adequacy]**

- (i) Upon formulating the aforementioned capital plan, whether the CO evaluates the adequacy of capital relative to the risks measured in comprehensive risk management conducted in consideration of changes in the business environment, etc.
- (ii) As for the amount of assets (e.g. the amount of net assets) to be held to prepare against business risks, which should not include financial sources procured for the purpose of preparing against credit risks and liquidity risks incurred in participant default, whether the CO has secured at least six months worth of operating expenditures, and examined

the sufficiency of the level of such amount in consideration of ensuring the CO's business continuity.

- (iii) Whether the CO properly examines equity capital, for example, as to whether the equity capital consists primarily of cash and cash equivalents, etc. and can thus be easily liquidated in a stress scenario.
- (iv) Whether the CO has a feasible plan to raise additional capital if the level of capital approaches or falls below levels that would make its business continuity uncertain.

### **III-2-2 Comprehensive Risk Management Framework**

#### **(1) Background and Objectives**

COs that intensively undertake processes after the execution of financial instruments transactions involving financial instruments face a wide range of risks, including not only credit risks and liquidity risks but also information technology risks and operational risks. COs are required to confirm whether such risks would affect the soundness of their financial condition, etc. and establish appropriate arrangements and procedures for risk management.

Also, in cases where financial institutions, etc. that are clearing participant provide money settlement and liquidity supply functions for COs, it is important that COs are aware that risks with such financial institutions, etc. will not be limited to the credit risks and that COs need to identify the risks with such financial institutions in a comprehensive manner.

#### **(2) Major Supervisory Viewpoints**

- (i) Whether the risk management division has sufficient authority, independence, resources, and access to the board in order to conduct effective risk management. For example, whether the reporting lines for risk management are clear and separate from those for other operations of the CO, so that the matters can be directly reported to the board of directors by the authority of the risk management division.
- (ii) Whether the CO has revealed and identified all risks in order to grasp diverse risks in a comprehensive manner, and if possible, has properly determined risk categories to place them under quantitative risk management.
- (iii) Whether the CO reviews the scope of quantification and accuracy to improve them as necessary. For example, whether the CO reviews the importance, correlation, etc. of different types of risks to ensure appropriateness.
- (iv) Whether the board of directors has clearly set up a policy for managing risks based on

strategic objectives in accordance with the management policy of the Clearing Organization as a whole, and examines the policy periodically, at least annually, and revises it as necessary. In addition, whether the board of directors takes appropriate measures to make the risk management policy widely known within the organization.

(v) Whether the board of directors makes use of risk-related information in the execution of business and the development of risk management systems by, for example, making necessary decisions based on risk status reports received periodically.

(vi) In cases where the money settlement functions are entrusted to a financial institution other than the BOJ, whether the Clearing Organization identifies the creditworthiness, capital, liquid assets and other conditions of such money-settling financial institution in a timely manner, and examines and controls risk management in a comprehensive manner in view of whether credit and liquidity risks are over-concentrated in such money-settling financial institution.

(vii) Whether the CO takes measures to identify and manage potential sources of risk arising from the set of contractual and operational arrangements among other financial market infrastructures that connect the CO directly or through an intermediary before entering into such arrangements, and on an ongoing basis once such arrangements are established.

### **III-2-3 Credit Risk Management**

#### **(1) Background and Objectives**

COs bear the risk of incurring losses from the deterioration in the financial position, failure of settlement, etc. on the part of the clearing participants, settlement banks, custodians and other parties to transactions in the course of payment and clearing.

Especially in the event of a participant default, etc., there is a possibility that rapid credit crunch, etc. among participants might give rise to serious turmoil in financial markets.

For this reason, COs are required to manage credit exposures to participants with precision, combine the margin system and other systems and techniques, limit potential losses that may arise from the settlement failure, etc. by participants and minimize their own losses as well as the losses of other participants.

#### **(2) Major Supervisory Viewpoints**

(i) Whether the CO has established a policy to manage credit risks that arise in the course of clearing operations conducted such as credit exposures to participants.

(ii) Whether the CO grasps its status of compliance with policies to identify the source of

credit risks, periodically measure the amount of credit risks and manage credit risks, and as necessary, takes measures such as reducing the amount of risks.

- (iii) Whether the CO takes measures to ensure the appropriateness, etc. of its credit risk management policy, such as utilizing participants and other outside experts as necessary, when formulating such policy. Whether the CO examines the appropriateness, etc. of the policy periodically, at least annually, according to changes in the external environment, etc. and revises it as necessary.
- (iv) Whether the CO covers credit exposures to participants with a high degree of confidence using margin and other prefunded financial resources. Specifically, whether the CO secures necessary prefunded financial resources by such means as implementing a margin system referred to in III-2-5.
- (v) Furthermore, whether the financial resources maintained, including additional financial resources, without limiting to prefunded financial resources, cover the stress scenario that includes the default of one participant (on a consolidated basis)<sup>(Note)</sup> that would potentially cause the largest aggregate credit exposure in consideration of extreme but plausible market conditions.

In particular, in cases where the CO is engaged in the clearing operations of instruments that involve complex risk profiles, such as credit default swaps (CDS), whether the financial resources maintained cover a more conservative scenario reflecting the complexity of such instruments, including the default of two participants (on a consolidated basis)<sup>(Note)</sup> that would potentially cause the largest aggregate credit exposure.

(Note) This refers to the amount calculated by including companies associated with such participant (meaning the subsidiaries and affiliates of said participant, parent of said participant, subsidiaries of said parent and affiliates of said parent).

- (vi) Whether the CO regularly tests the sufficiency of the aforementioned necessary financial resources through rigorous stress testing, etc., while taking into consideration the following points.
  - A. In conducting stress testing, whether there is a spectrum of forward-looking stress scenarios which take into considerations a variety of extreme but plausible market conditions, such as changes in market factors including price volatilities and yield curves, default of multiple participants, and pressure in markets in the event of participant default.
  - B. Whether the CO conducts stress testing and backtesting on a daily basis using predetermined scenarios, models, parameters, etc. according to its risk management



policy. Whether the CO has formulated clear procedures to report the test results to the appropriate decision makers in the CO, evaluate the sufficiency of financial resources, and secure additional resources as necessary.

- C. Whether the CO analyzes the appropriateness of the adopted scenarios, models, parameters, etc. in detail on at least a monthly basis. Whether the CO analyzes the scenarios, etc. more frequently if it is deemed necessary to do so when, for example, market volatility increases, liquidity decreases, or the size or concentration of positions held by participants increases significantly.
- D. Whether the CO performs a full validation of its risk-management model and revises the model as necessary at least annually, in conjunction with the examination of its policy to manage the aforementioned risks.

### **III-2-4 Liquidity Risk Management**

#### **(1) Background and Objectives**

When a counterparty to a transaction cannot make the settlement by the due date, even though the counterparty may perform its obligation at some point in the future, the CO will incur a loss due to the nonperformance of such obligation (liquidity risk).

In such cases, the CO has to complete the settlement with its own liquid assets to cover the shortfall in funds arising from the failure of such obligation with its own liquid assets; COs are thus required to manage liquidity risks with precision by such means as identifying liquidity risks and securing liquid assets commensurate with such risks.

#### **(2) Major Supervisory Viewpoints**

- (i) Whether the CO has established a policy to manage liquidity risks that arise in the course of clearing operations conducted. Whether the CO has effective operational and analytical tools to monitor its settlement and funding flows on an ongoing and timely basis.
- (ii) Whether the liquidity resources maintained in all relevant currencies, cover the stress scenario that includes the default of one participant (on a consolidated basis)<sup>(Note)</sup> that requires the most liquid resources, in consideration of extreme but plausible market conditions.

In particular, in cases where the CO is engaged in the clearing operations of instruments that involve complex risk profiles, such as CDS, whether the liquid assets cover a more conservative scenario reflecting the complexity of such instruments, including the defaults of two participants (on a consolidated basis)<sup>(Note)</sup> that require the

most liquid resources.

(Note) This refers to the amount calculated by including companies associated with such participant.

- (iii) Whether the CO limits liquid assets to deposits with the BOJ and financial institutions, commitment lines or others subject to a prearranged funding arrangement which can be immediately used and cashed in the event of an emergency.
- (iv) Whether the CO sufficiently confirms that the provider of liquid assets has the capacity to provide liquidity based on the prearranged arrangement, such as by having established arrangements and procedures to manage its own liquidity risk with precision.
- (v) In cases where the CO has access to the BOJ's accounts, payment services and securities settlement services, if practical, whether the CO uses such services to enhance its management of liquidity risks.
- (vi) Whether the CO regularly tests the sufficiency of the aforementioned liquid financial resources through rigorous stress testing, while taking into consideration the following points.
  - A. In conducting stress testing, whether there is a spectrum which takes into consideration a variety of extreme but plausible market conditions, such as changes in market factors including price volatilities and yield curves, default of multiple participants, and pressure in markets in the event of participant default.
  - B. Whether the CO conducts stress testing on a daily basis using predetermined scenarios, models, parameters, etc. according to its risk management policy. Whether the CO has formulated clear procedures to report the test results to the appropriate decision makers in the CO, evaluate the sufficiency of financial resources and secure additional resources as necessary.
  - C. Whether the CO analyzes the appropriateness of the adopted scenarios, models, parameters, etc. in detail on at least a monthly basis. Whether the CO analyzes the scenarios, etc. more frequently if it is deemed necessary to do so when, for example, market volatility increases, liquidity decreases, or the size or concentration of positions held by participants increases significantly.
  - D. Whether the CO performs a full validation of its risk-management model overall and revises the model as necessary at least annually, in conjunction with the examination of its policy to manage the aforementioned risks.

### **III-2-5 Margin System**

#### **(1) Background and Objectives**

Margins are for preparing against rapid fluctuations in the position due to such events as participant default, in addition to daily exposures arising from market price fluctuations, etc., based on an appropriate combination of variation margin and initial margin, etc.

An effective margin system performs an important role in credit and liquidity risk management of COs. COs are required to develop and examine a margin system that calculates margin levels based on the risk profiles, etc. of financial instruments subject to clearing, in consideration of stressed market conditions such as in the event of participant default.

## **(2) Major Supervisory Viewpoints**

- (i) Whether the CO has a margin system that calculates margin levels based on the risk profiles, etc. of financial instruments subject to clearing.
- (ii) Whether the CO takes measures to ensure the appropriateness, etc. of the margin system such as utilizing participants and other outside experts as necessary when developing and reviewing the margin system.
- (iii) Whether the CO has established arrangements and procedures to obtain the latest data to properly calculate the margin. Also, whether there are predetermined policies to evaluate and determine the price in a reasonable manner in cases where objective price information is difficult to obtain from outside due to market characteristics and other such factors.
- (iv) Whether the CO has adopted appropriate scenarios, models, parameters, etc. according to the risk profiles, etc. of financial instruments. In particular, whether the CO has secured at least five days for OTC derivatives, at least two days for other OTC instruments and at least one day for listed instruments as the liquidation period presumed in the models, and whether the CO verifies whether said period is conservative in consideration of the risk profiles, etc. of financial instruments, among others. Also, in cases where historical data is used for market fluctuation parameters, whether the sample period for historical data used in the calculation is adequate in light of past market fluctuations, etc.
- (v) Whether the CO confirms that the initial margin that has been calculated is at an adequate level, at least covering a single-tailed confidence level of 99 percent with respect to the estimated distribution of losses.

(Note) If margin is calculated at the portfolio level, whether the CO confirms that margin is at an adequate level, at least covering single-tailed confidence level of 99 percent with respect to the estimated distribution of losses, while taking into consideration whether it is sufficiently reasonable to allow offsets of risks

within the portfolio and perform margin reductions with respect to each portfolio's distribution of future exposure.

- (vi) When calculating the variation margin, whether the CO marks participant positions to market and collects variation margin frequently, at least daily. Whether the CO has the authority to make intraday margin calls to clearing participants if necessary, and has established arrangements and procedures to do so.
- (vii) With respect to the margin calculation model, etc., whether the CO conducts backtesting at least daily, analyzes the performance, etc. of the margin calculation model at least monthly, and performs a full validation of the model and revises the model as necessary at least annually, according to its risk management policy.

Whether the aforementioned annual validation and as-needed revisions are to be carried out consistently with the examination of arrangements and procedures for risk management referred to in III-2-2.

### **III-2-6 Collateral System**

#### **(1) Background and Objectives**

Collateral is significant in that it not only reduces the credit risks borne by CO by protecting their credit exposures but also gives participants the incentive to manage risks.

On the other hand, the liquidation value of collateral varies with market conditions, so under stressed market conditions such as in the event of participant default, market price and liquidity may rapidly fall.

For this reason, COs need to apply prudent haircuts to the value of the collateral so that the liquidation value of the collateral under stressed market conditions would be equal to or greater than the amount subject to protection, and establish arrangements and procedures so that the collateral can actually be disposed of under stressed market conditions.

#### **(2) Major Supervisory Viewpoints**

- (i) Whether the CO generally limits the assets it accepts as collateral to those with low credit, liquidity, and market risks.
- (ii) Whether the CO develops haircuts by establishing prudent collateral valuation practices. Whether the haircuts are regularly tested and take into account stressed market conditions.
- (iii) In order to reduce the need for procyclical adjustments, whether the CO establishes stable and conservative haircuts that are calibrated to include periods of stressed market conditions, to the extent practicable and prudent.

(iv) Whether the CO takes measures to avoid concentrated holdings of certain assets as collateral.

(v) Whether the CO that accepts foreign collateral mitigates the risks associated with its use and ensures that the collateral can be used in a timely manner.

### **(3) Supervisory Method and Actions**

The right prescribed in Article 68(1)(iii) of the Cabinet Office Order on Financial Instruments Exchanges (hereinafter referred to as "LG") is recognized as substitute securities, etc. for clearing margins. It should be noted that LG is exceptionally permitted as substitute securities, etc., in light of the following points:

-There is a strong need for financial instruments business operators, etc. that conduct specified currency-related over-the-counter derivatives transactions (meaning specified currency-related over-the-counter derivatives transactions prescribed in Article 117(1)(xxviii)-2 of the Cabinet Office Order on Financial Instruments Business; the same applies hereinafter) to promote the use of COs in order to stably conduct specified currency-related over-the-counter derivatives transactions and a cover deal (meaning the cover deal prescribed in Article 94(1)(i) of said order; the same applies hereinafter)

-It is effective to allow financial instruments business operators, etc. that conduct specified currency-related over-the-counter derivatives transactions to use LG as substitute securities, etc. as an incentive to promote the use of COs.

Based on this, the use of LG should be reviewed as necessary in light of changes in the market environment, etc.

## **III-2-7 Development of Recovery Plans**

### **(1) Background and Objectives**

When a CO faces a crisis, not only the CO itself but also the financial system as a whole is likely to face a severe disruption. Thus, at the international level, an agreement at the Financial Stability Board (see the following note 1) calls on jurisdictions to put in place a process to develop robust and credible "Recovery and Resolution Plans (RRPs)." In addition, regarding recovery plans, CPMI-IOSCO provides guidance in a report (see the following note 2).

COs in Japan are not considered to be "systemically important CO in multiple jurisdictions" as determined by CPMI-IOSCO and relevant authorities. In addition, COs have taken measures, such as stipulating in their business rules that, in order to ensure the appropriate performance of financial instruments obligation assumption services, clearing participants shall bear all losses in the event of losses (Article 156-10 of the FIEA). However, in order to ensure the stability of

the financial system, it is necessary to continue efforts toward the formulation of recovery plans. Once any CO in Japan becomes a systemically important CO in multiple jurisdictions, additional measures will be considered.

(Note 1) Financial Stability Board, “Key Attributes of Effective Resolution Regimes for Financial Institutions,” November 2011; Financial Stability Board, “Resolution of Financial Market Infrastructures (FMIs) and FMI Participants,” October 2014; Financial Stability Board, “Guidance on Central Counterparty Resolution and Resolution Planning” July 2017

(Note 2) CPMI-IOSCO, “Recovery of financial market infrastructures” October 2014 (revised in July 2017)

## **(2) Major Supervisory Viewpoints**

The FSA expects to require, pursuant to Article 156-15 of the FIEA, COs for which obligations based on transactions listed in the items of Article 156-62 of the FIEA are subject to their financial instruments obligation assumption service to develop and submit a recovery plan once a year or when important changes have been made to their business and group structure. Taking note that the contents of a recovery plan could vary depending on the group structure or the business model of the CO, the FSA expects to examine whether a recovery plan contains at least the items listed below:

- (i) Outline of the recovery plan
  - A. Relevance of the recovery plan for the CO; and
  - B. Governance arrangements to develop the recovery plan;
- (ii) Preliminary information for developing the recovery plan
  - A. Overviews of the business and the group structure; and
  - B. Risk management systems in normal times with respect to capital adequacy and liquidity;
- (iii) Triggers for the implementation of the recovery plan
  - A. Identification of trigger events that are expected to be hit at a stage sufficiently early enough for the CO to respond to the crisis preemptively (including quantitative and qualitative triggers with respect to each of capital adequacy and liquidity);
  - B. Stress tests and reverse stress tests with severer stress than for usual stress testing (including system-wide and firm-specific stress scenarios);
  - C. Internal decision-making process concerning both a judgment of the trigger(s) being hit and actions to be taken thereafter; and
  - D. Relationship between risk management operations in business as usual depending on crisis stages and those at the time of the recovery plan being implemented;

(iv) Analysis of recovery options

- A. Assessment of effectiveness, appropriateness and sufficiency (including quantitative assessment) of recovery options (measures to improve the capital situation and those to secure sufficient liquidity) for each of the stress scenarios; and
- B. Points to be taken into account during the execution of the recovery options and the feasibility analysis thereof;

(v) Other items

A. Management information systems

List of information necessary for development of the recovery plan and implementation of the recovery options, and the time needed to access those information

### **III-2-8 Supervisory Method and Actions**

In cases where a problem has been found in the soundness of the financial condition or the status of the risk management arrangements and procedures of a CO, the supervisory departments shall monitor voluntary business improvement made by the CO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-15 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 156-16 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting public interests and investors.

### **III-3 Operational Appropriateness**

#### **III-3-1 Compliance**

##### **III-3-1-1 Measures for Ensuring Compliance**

###### **(1) Notes Regarding Policies, Procedures, etc. Pertaining to Compliance**

- (i) Whether the CO regards compliance as one of the most important issues for management, and whether it has formulated a basic policy concerning the implementation of compliance, as well as a detailed implementation plan (compliance program) and a code of conduct (ethics code, compliance manual), etc.
- (ii) Whether the CO has clearly established the authority and responsibility of the chief compliance officer, and whether there is a system in place for his/her function to be fully exercised.
- (iii) Whether the CO has established a system for communicating and reporting compliance-related information appropriately among the management team, the divisions in charge of the clearing operations, and the compliance division, chief compliance officer or other person in charge.

###### **(2) Notes Regarding Whistle-blowing System**

- (i) Whether the CO has clearly designated the division in charge of the whistle-blowing system and established specific procedures for handling internal allegations, so as to ensure that they are processed and a response is made in a prompt and appropriate manner.
- (ii) Whether the CO has developed a system wherein information on the content of internal allegations can be shared within a necessary and appropriate scope.
- (iii) Whether the CO makes sure to properly follow up on how internal allegations are being handled.
- (iv) Whether the CO accurately and appropriately records and stores the details of internal allegations and the results of investigations thereof, and whether it makes full use of this information such as to improve its operational control system and to formulate measures for preventing a recurrence.

##### **III-3-1-2 Fair Participation Requirements, etc.**

###### **(1) Background and Objectives**



Given the role of COs, which is to contribute to the stable and efficient business operations of market participants by intensively executing processes, etc. in financial transactions, COs' services should be fair and open to participants, other COs, etc.

At the same time, COs are required to establish reasonable risk-related participation requirements and manage risks of participants to which COs are exposed, in order to ensure their own financial soundness and provide clearing services in a stable manner.

## **(2) Major Supervisory Viewpoints**

- (i) Whether the CO has established reasonable risk-related participation requirements for participants.
- (ii) Whether the CO examines whether such participation requirements are fair or not from the viewpoint of providing clearing services in a stable manner, etc. in the market of operations subject to clearing, and releases the participation requirements to the public in consideration of such examination.
- (iii) Whether the CO abuses its position in such circumstance as using information received from clearing operations in other services and concluding contracts on services incidental to clearing operations.
- (iv) Whether the CO monitors compliance with its participation requirements on an ongoing basis such as receiving reports on the financial position, etc. from participants in a timely manner. Whether the CO has clearly defined and publicly disclosed procedures for facilitating the suspension and exit of clearing participants who no longer meet the participation requirements.

## **(3) Supervisory Method and Actions**

In cases where a problem has been found in the participation requirements or compliance monitoring, the supervisory departments shall monitor voluntary business improvement made by the CO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-15 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 156-16 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting public interests and investors.

### **III-3-1-3 Prevention of Damage that May be Inflicted by Anti-Social Forces**

#### **(1) Background and Objectives**

Eliminating anti-social forces from society is a task critical to ensuring the order and safety of society, so it is necessary and important to promote efforts to ban any relations with anti-social forces from the viewpoint of fulfilling social responsibility. In particular, as COs are highly public in nature and play an important economic role, they need to exclude anti-social forces from financial instruments markets in order to prevent damage from being inflicted not only on itself and their officers and employees but also on various stakeholders who participate in financial instruments markets.

Needless to say, if COs are to retain public confidence and maintain the soundness and appropriateness of their business operations, it is essential that they deal with anti-social forces in accordance with laws and regulations without bowing to pressure from them. Therefore, COs must strive, on a daily basis, to develop a control environment for banning any relations with anti-social forces in accordance with the purpose of the “Guideline for How Companies Prevent Damage from Anti-Social Forces” (agreed upon at a meeting on June 19, 2007 of cabinet ministers responsible for anti-crime measures).

In particular, anti-social forces have become increasingly sophisticated in their efforts to obtain funds, disguising their dealings as legitimate economic transactions through the use of affiliated companies in order to develop business relations with ordinary companies. In some cases, the relations thus developed eventually lead to problems. In order to deal with such cases properly, the management teams of COs need to take a resolute stance and implement specific countermeasures.

It should be noted that if a CO delays specific actions to resolve a problem involving anti-social forces on the grounds that unexpected situations, such as the safety of officers and employees being threatened, could otherwise arise, the delay could increase the extent of the damage that may be ultimately inflicted on the CO.

(Reference) “Guideline for How Companies Prevent Damage from Anti-Social Forces”  
(agreed upon at a meeting on June 19, 2007 of cabinet ministers responsible  
for anti-crime measures)

**(i) Basic Principles on Prevention of Damage that may be Inflicted by Anti-social Forces**

- Institutional response
- Cooperation with external expert organizations
- Ban on any relations, including transactions, with anti-social forces
- Legal responses, both civil and criminal, in the event of an emergency
- Prohibition of engagement in secret transactions with and provision of funds to anti-social forces

## **(ii) Identification of Anti-social Forces**

In judging whether specific groups or individuals constitute “anti-social forces,” which are defined as groups or individuals that pursue economic profits through the use of violence, threats and fraud, it is necessary not only to pay attention to whether they fit the definition in terms of their affiliation, such as whether they constitute or belong to *boryokudan* crime syndicates, *boryokudan* affiliated companies, *sokaiya* racketeer groups, groups engaging in criminal activities under the pretext of conducting social campaigns or political activities and crime groups specialized in intellectual crimes, but also to whether they fit the definition in terms of the nature of their conduct, such as whether they are making unreasonable demands that go beyond the limits of legal liability. (Refer to the “Key Points of Measures against Organized Crime,” a directive issued in the name of the Deputy Commissioner-General of the National Police Agency on December 22, 2011.)

## **(2) Major Supervisory Viewpoints**

A CO should not have any relations with anti-social forces and, in cases where it has established a relationship with an anti-social force unwittingly, supervisors, while also giving consideration to the characteristics of specific transactions, shall pay attention to such as the following points in order to examine its control environment for banning any relations with anti-social forces as soon as possible after the counterparty has been found to be an anti-social force and its control environment for dealing with unreasonable demands by anti-social forces appropriately.

### **(i) Institutional response**

In light of the need and importance of an action to ban any relationship with anti-social forces organically, whether the responsibility of responding to the situation is not left solely to the relevant individuals or divisions but the management including directors are appropriately involved, and there is a policy for the entire organization to respond. In addition, whether there is a policy calling for the corporate group as a whole, not just the involved CO alone, to take on an effort to prevent any relationship with anti-social forces. Furthermore, whether the CO is also making efforts to eliminate anti-social forces when conducting transactions including the provision of financial services under business alliance with other companies outside of the corporate group.

### **(ii) Developing of a Centralized Control Environment through anti-social forces response division**

Whether the CO has established a division in charge of supervising responses to ban

any relationship with anti-social forces (hereinafter referred to as the “anti-social forces response division”) so as to develop a centralized control environment for preventing anti-social forces from inflicting damage, and whether this division is properly functioning.

In particular, whether the CO pays sufficient attention to the following points in developing the centralized control environment.

- A. Whether the anti-social forces response division is actively collecting and analyzing information on anti-social forces and has developed a database to manage such information in a centralized manner and further, has a system to appropriately update it (i.e., addition, deletion or change of information in the database). Further, whether the division is making efforts to share information within the group in the process of collecting and analyzing such information. Whether the anti-social forces response division has a system to appropriately take advantage of such information for screening counterparties of transactions and evaluating the attributes of shareholders of the CO.
- B. Whether the CO makes sure to maintain the effectiveness of measures to ban any relations with anti-social forces by, for example, having the anti-social forces response division develop a manual for dealing with anti-social forces, provide on-going training, foster cooperative relationships with external expert organizations such as the police, the National Center for the Elimination of Boryokudan and lawyers on an ongoing basis. In particular, whether the CO is prepared to report to the police immediately when it faces the imminent prospect of being threatened or becoming the target of an act of violence, by maintaining close communications with the police on a daily basis so as to develop a systematic reporting system and build a relationship that facilitates cooperation in the event of a problem.
- C. Whether the CO has a structure in which relevant information is appropriately conveyed to the anti-social forces response division for consultation when transactions with anti-social forces are found or such forces have made unreasonable demands. Further, whether the anti-social forces response division has a structure to appropriately report relevant information to the management. In addition, whether the anti-social forces response division has a structure to ensure the safety of individuals encountering anti-social forces in person and to support divisions involved in dealing with them.

**(iii) Execution of Appropriate Prior Screening**

Whether the CO bans allowing anti-social forces to become a participant or

counterparty to a transaction by conducting appropriate advance screening using information on such forces in order to prevent transactions with anti-social forces, and makes sure provisions regarding the exclusion of “boryokudan” crime syndicates are introduced in all contracts and terms of transactions.

**(iv) Execution of Appropriate Follow-up Review**

Whether, for the purpose of making sure any relationships with anti-social forces are eliminated, there is a structure to conduct an appropriate follow-up review on existing claims and contracts.

**(v) Measures to Terminate Transactions with Anti-Social Forces**

- A. Whether the CO has a system under which information confirming the existence of a transaction with anti-social forces is appropriately reported to the management, including directors, etc., via the anti-social forces response division, and responds to the situation under appropriate directions and involvement by the management.
- B. Whether the CO regularly communicates with external expert organizations, including the police, the National Center for the Elimination of Boryokudan, lawyers and so forth, and promotes efforts to eliminate any transactions with anti-social forces.
- C. Whether the CO, when it has learned through a follow-up review after initiating a transaction that the counterparty is a member of an anti-social force, takes measures to prevent the provision of benefits to anti-social forces, such as seeking collection to the extent possible.
- D. Whether the CO has a structure to prevent providing funds or engaging in inappropriate or unusual transactions for whatever reason if the counterparty has been found to be an anti-social force.

**(vi) Dealing with Unreasonable Demands by Anti-Social Forces**

- A. Whether the CO has a system under which the information that anti-social forces have made unreasonable demands is immediately reported to the management, including directors, etc., via the anti-social forces response division and responds to the situation under appropriate directions and involvement by the management.
- B. Whether the CO actively consults external expert organizations such as the police, the National Center for the Elimination of Boryokudan, and lawyers, when anti-social forces make unreasonable demands, and responds to such unreasonable demands based on guidelines set by the National Center for the Elimination of Boryokudan and other organizations. In particular, whether the CO has a structure to report to the police immediately when there is an imminent prospect of a threat being made or an act of violence being committed.
- C. Whether the CO, in response to unreasonable demands by anti-social forces, has a

policy to take every possible civil legal action and to avoid hesitating to seek the initiation of a criminal legal action by proactively reporting damage to the authorities.

D. Whether the CO ensures that the division in charge of handling problematic conduct promptly conducts a fact-finding investigation upon request from the anti-social forces response division, in cases where the unreasonable demand from anti-social forces is based on problematic conduct related to business activity or involving an officer or employee.

**(vii) Management of Shareholder Information**

Whether the CO manages shareholder information properly, through means such as checking the transaction status of its own shares and examining information regarding the attributes of its shareholders.

**(3) Supervisory Method and Actions**

When supervisory departments have recognized an issue of supervisory concern regarding a CO's control environment for banning any relations with anti-social forces, through inspection and daily supervisory administration, they shall identify and keep track of the status of voluntary improvement made by the CO by holding in-depth hearings and, when necessary, requiring the submission of reports based on Article 156-15 of the FIEA. When the CO is deemed to have a serious problem from the viewpoint of protecting public interests and investors, because its internal control environment is extremely fragile, as shown by, for example, a failure to take appropriate steps toward dissolving relations with anti-social forces despite recognizing the provision of funds thereto and the presence of inappropriate business relations therewith, supervisory departments shall take actions such as issuing an order for business improvement based on Article 156-16 of the FIEA.

**III-3-2 Business Continuity Management (BCM)**

**(1) Background and Objectives**

COs assume the liabilities of financial instruments intensively and settle transactions in large amounts. They are required to take such actions as formulating an appropriate business continuity plan (BCP) in order to recover their operations as soon as possible and continue their operations even in the event of an emergency, e.g., acts of terrorism, large-scale disasters.

**(2) Major Supervisory Viewpoints**

(i) Whether the CO recognizes what constitutes an emergency and is striving as much as

- possible to prevent or guard against any emergency by, for example, conducting inspections and anti-crisis practices periodically in normal times.
- (ii) Whether the CO formulates emergency response policies, etc., including a BCP, to recover their operations as soon as possible and continue their operations even in the event of an emergency, and periodically reviews them. In particular, whether the CO clarifies its decision making system in crises.
  - (iii) Whether the board of directors clearly defines the roles and responsibilities for addressing an emergency and endorses the CO's operational risk-management framework in the case of formulating and significantly changing the emergency response policies, etc.
  - (iv) Whether the BCP, etc. aims to resume the operation of the indispensable information system within two hours from system halt and to complete settlement on the same day on which the fault occurred.
  - (v) Whether the CO has developed a control environment for promptly making a report to the Financial Markets Division of the Policy and Markets Bureau of the FSA and making relevant organizations within the CO work closely with each other if an emergency has arisen or if the possibility of an emergency has been recognized.
  - (vi) Whether the CO has established a backup center while taking geographic factors into account as a safety measure to prepare against emergencies. Whether the CO backs up business data in a timely manner and periodically conducts drills such as switching over to the backup center.
  - (vii) Whether the CO has considered measures assuming the possibility of electricity supply, communication lines, public transport and other social infrastructures coming to a halt.

### **(3) Supervisory Method and Actions**

When supervisory departments have recognized an issue of supervisory concern regarding a CO's control environment for crisis management, through daily supervisory administration, etc., they shall identify and keep track of the status of voluntary improvement made by the CO by holding in-depth hearings and, when necessary, requiring the submission of reports based on Article 156-15 of the FIEA.

When supervisory departments have recognized the occurrence of an emergency or the likelihood of an emergency occurring, they shall hold hearings periodically and check the situation first-hand so that they can identify and keep track of how the relevant CO is responding to the emergency, including whether the response (status of the development of a control environment for crisis management, securement of clearing functions, communications with relevant parties including participants, dissemination of information,

etc.) is sufficient in light of the level and type of the emergency, until the situation improves. In addition, they shall require the submission of a report based on Article 156-15 of the FIEA when necessary.

### **III-3-3 Operational Risk Management**

#### **(1) Background and Objectives**

Operational Risk is the risk of COs, etc. incurring losses due to their officers and employees failing to conduct administrative work properly, causing accidents or committing illegal acts in the course of the administrative work process, and is deemed to be caused by various factors such as information systems and internal procedures, in addition to human errors.

It is important that COs pursue sound and appropriate business operations by establishing arrangements and procedures for managing operational risks.

#### **(2) Major Supervisory Viewpoints**

- (i) Whether the CO has established appropriate policies, procedures, etc. to identify and manage operational risks. Whether the CO examines them periodically, and reviews them as necessary. Whether the board of directors endorses such policies, procedures, etc., and clearly defines the roles and responsibilities for addressing operational risk. Also, whether the CO has implemented specific measures to reduce operational risks.
- (ii) Whether the CO has sufficient processing capacity to achieve a certain level of service in consideration of the volume of administrative processes, etc. expected in the future.
- (iii) In cases where the CO outsources part of its administrative processes to service providers or other third parties or relies on them, whether the CO confirms that the outsource fulfills the requirements that would have to be met if such processes were carried out by the CO itself.
- (iv) Whether the CO has specified a policy and procedures for selecting the business operations to be outsourced and the contractors to outsource them to, and concluded a contract and developed a control environment that enables sufficient management of such contractors.

#### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the response by the CO, the supervisory departments shall monitor voluntary business improvement made by the CO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when



necessary, requiring the submission of a report based on Article 156-15 of the FIEA.

Furthermore, the supervisory departments shall take actions such as issuing an order for business improvement based on Article 156-16 of the FIEA, when the CO's control environment for managing operational risks is deemed to have a serious problem and the action is deemed to be necessary and appropriate from the viewpoint of protecting public interests and investors.

### **III-3-4 Information Technology Risk Management**

#### **(1) Background and Objectives**

Information technology risk is the risk that COs, etc. will incur losses generally because of a computer system breakdown, malfunction or other inadequacies, or because of inappropriate or illegal use of computer systems.

COs' systems are themselves market infrastructures that are indispensable for clearing, etc., so if any system troubles or cybersecurity incidents occur, they may inflict damage on COs and participants connected to the systems, and in turn, impact the financial system as a whole.

Therefore, it is important to build a robust control environment for managing information technology risks in COs.

(Note) "Cybersecurity incidents" refers to instances of cybersecurity being threatened by so-called cyberattacks, including unauthorized intrusion, theft, modification and destruction of data, failure or malfunction of information systems, execution of illegal computer programs and DDoS attacks, committed via the Internet through malicious use of information communication networks and information systems.

#### **(2) Major Supervisory Viewpoints**

##### **(i) Recognition of Information Technology Risk**

- A. Whether the board of directors has formulated a basic policy for company-wide management of information technology risk based on a full recognition of information technology risk.
- B. Whether the board of directors recognizes that prevention and efforts for speedy recovery from system troubles and cybersecurity incidents (hereinafter referred to as "system trouble, etc.") is an important issue and has developed an appropriate control environment.
- C. Whether there are arrangements and procedures for ensuring that information regarding information technology risk is properly reported to the management team.

##### **(ii) Establishment of Appropriate Control Environment for Risk Management**

- A. Whether the CO has specified a basic policy for the management of information technology risk and developed a relevant control environment.
- B. Whether the CO has designated the types of risk that should be managed according to specific criteria and has identified the location of the risk.
- C. Whether the control environment for managing information technology risk is effective enough to, enable the CO to identify and analyze the actual state of its

business operations and system troubles, and minimize the frequency and scale of system troubles in a manner suited to the system environment and other factors, thereby maintaining an appropriate level of computer system quality.

**(iii) Assessment of information technology risk**

Whether the division managing information technology risk recognizes and assesses risks periodically or in a timely manner by recognizing the fact that risks are becoming diversified due to changes in the external environment, such as seen in the examples of system troubles induced by large-scale transactions as a result of increased customer channels and efforts to enhance information networks that bring more diverse and broad-based impacts.

Also, whether it is taking sufficient measures to address the risks that have been identified.

**(iv) Management of information security**

A. Whether the CO has developed a policy to appropriately manage information assets, prepared organizational readiness, introduced in-house rules, etc., and developed an internal control environment. Also, whether it is making continuous efforts to improve its information security control environment through the PDCA cycle, taking notice of illegal incidents or lapses at other companies.

B. Whether the CO is managing information security by designating individuals responsible for it and clarifying their roles/responsibilities in efforts to maintain the confidentiality, integrity and availability of information. Also, whether the individuals responsible for information security are tasked to handle the security of system, data and network management.

C. Whether the CO is taking measures to prevent unauthorized use of computer systems, unauthorized access, and intrusion by malicious computer programs such as computer viruses.

D. Whether the CO identifies important information of participants it is responsible for protecting in a comprehensive manner, keeps its records and manages them.

Whether the CO, in identifying important information of participants, has set business operations, systems and external contractors as the scope of protection and includes data, such as listed below, in the scope where it tries to identify those calling for protection.

- Data stored in the areas within the system that are not used in ordinary operations
- Data output from the system for analyzing system troubles, etc.

E. Whether the CO is assessing importance and risks regarding important information of participants that has been identified.

Also, whether it has developed rules to manage information, such as those listed below, in accordance with the importance and risks of each piece.

- Rules to encrypt or mask information
- Rules for utilizing information
- Rules on handling data storage media, etc.

F. Whether the CO has introduced measures to discourage or prevent unauthorized access, unauthorized retrieval, data leakage, etc. such as listed below, for important information of participants.

- Provision of access authorizations that limits access to the scope necessary for the person's responsibility
- Storage and monitoring of access logs
- Introduction of mutual checking functions such as by separating the individuals in charge of development and those responsible for operations, administrators and those responsible for operations, etc.

G. Whether the CO has introduced rules for controlling confidential information, such as encryption and masking. Also, whether it has introduced rules regarding the management of encryption programs, encryption keys, and design specifications for encryption programs.

Note that "confidential information" refers to information, such as PIN, passwords, etc., whose misuse could lead to losses by participants.

H. Whether the CO gives due consideration to the necessity of holding/disposing of, restricting access to, and taking outside, of confidential information, and treats such information in a stricter manner.

I. Whether the CO periodically monitors its information assets to see whether they are managed properly according to management rules, etc. and reviews the control environment on an ongoing basis.

J. Whether the CO conducts security education (including by external contractors) to all officers and employees in order to raise awareness of information security.

**(v) Management of cybersecurity**

A. Whether the board of directors, etc. recognizes the importance of cybersecurity amid increasingly sophisticated and cunning cyberattacks and has introduced the necessary control environment.

B. Whether the CO has introduced systems to maintain cybersecurity, such as listed below, in addition to making the organization more secure and introducing in-house rules, etc.

- Monitoring systems against cyberattacks

- Systems to report cyberattacks and public-relation systems when attacks occur
- Emergency measures by Computer Security Incident Response Teams and systems for early detection

- Systems of information collection and sharing through information-sharing organizations, etc.

C. Whether the CO has introduced a multi-layered defence system against cyberattacks that combines security measures respectively for inbound perimeter control, internal network security control and outbound perimeter control.

- Security measures for inbound perimeter control (e.g. introduction of a firewall, anti-virus software, Intrusion Detection System, Intrusion Protection System etc.)

- Security measures for internal network security control (e.g. proper management of privileged IDs/passwords, deletion of unnecessary IDs, monitoring of execution of certain commands, etc.)

- Security measures for outbound perimeter control (e.g. retrieval and analysis of communication/event logs, detecting/blocking inappropriate communication, etc.)

D. Whether measures such as listed below are implemented to prevent damage from expanding when cyberattacks occur.

- Identification of IP addresses from which the cyberattacks originate and blocking off of attacks

- Functions to automatically spread out accesses when under DDoS attacks

- Suspension of the entire system or its part, etc.

E. Whether necessary measures for vulnerabilities in the system, such as updating of the operating system and application of security patches, are introduced in a timely manner.

F. Whether the CO is, as part of cybersecurity measures, assessing its security levels by taking advantage of tests on network intrusion, vulnerability scanning or penetration tests, etc. and making efforts to improve security.

G. Whether the CO, when carrying out business operations using communication methods such as the Internet, has introduced appropriate authentication methods in line with the risks associated with such transactions, such as listed below.

- Authentication methods that do not rely on fixed IDs or passwords, such as variable passwords and digital certificates

- Transaction authentication using transaction signatures by means of a hardware token, etc.

H. Whether the CO, when carrying out business operations using communication methods such as the Internet, has introduced preventative measures in line with

operations, such as listed below.

-Introduction of software that allows the CO to detect virus infection of the participant's PC and issue a warning

-Adoption of methods to store digital certificates in mediums or devices separate from PCs used in the relevant business operation, such as IC cards

-Introduction of a system that allows the CO to detect unauthorized log-ins, abnormal input, etc. and immediately notify such abnormalities to participants

I. Whether the CO has developed contingency plans against potential cyberattacks, conducts exercises and reviews such plans. Also, whether it participates in industry-wide exercises as necessary.

J. Whether the CO has formulated plans to train and expand the personnel responsible for cybersecurity and implements them.

**(vi) System Planning, Development and Operational Management**

A. Whether the CO has formulated a medium/long-term development plan after having clarified its strategic policy for systems as part of its management strategy. Whether the medium/long-term development plan has been approved by the board of directors.

B. Whether the CO reveals the risks inherent to its existing systems on an ongoing basis, and makes investments to maintain and improve the systems in a planned manner.

C. Whether the CO has clarified its rules for approval of plans, development and transition in development projects.

D. Whether the CO specifies the responsible person with respect to each development project and manages the progress based on the development plan.

E. Upon system development, whether the CO conducts tests in an appropriate and sufficient manner, such as by preparing test plans and making user divisions participate.

F. For human resources development, whether the CO formulates and implements specific plans to pass on the mechanism and development technologies of its existing systems and train personnel with expertise.

**(vii) Computer System Audits**

A. Whether an internal audit section that is independent from the computer system division conducts periodic audits of the computer system.

B. Whether the CO conducts internal audits by subject matter about computer systems and is taking of external audits by information system auditors.

C. Whether the audited division accounts for all business operations involving information technology risk.

**(viii) Management of Outsourcing of Business Operations**

- A. Whether the CO selects outsources (including system subsidiaries) by evaluating and examining them based on selection criteria.
- B. Whether the CO has prescribed the allocation of roles and responsibilities, audit authority, subcontracting procedures, level of services rendered, etc. with the outsource in an outsourcing agreement. Also whether the CO presents to outsourced contractors rules their employees are required to adhere to and security requirements, as well as defines them in contract forms, etc.
- C. Whether the CO properly conducts risk management regarding outsourced business operations (including work further subcontracted) related to the computer system. In cases where system-related administrative processes are outsourced, whether the CO properly conducts risk management according to the outsourced business operations related to the computer system.
- D. Whether the CO periodically monitors the outsourced business operations (including work further subcontracted) to determine, as the outsourcer, that the outsourced business operations are properly conducted.  
Also, whether there is a system that allows the consigner to monitor and track the status of data of investors and participants being processed at outsourced contractors.

**(ix) Contingency Plan**

- A. Whether the CO has formulated a contingency plan and has established arrangements and procedures for dealing with emergencies.
- B. Whether the CO is basing the details of its contingency plan on guides that allows it to judge objective levels of its details (such as "Guide to Formulate Contingency Plans at Financial Institutions" compiled by the Center for Financial Industry Information Systems).
- C. Whether the CO, in developing a contingency plan, assumes not only contingencies due to natural disasters but also system troubles, etc. due to internal or external factors.  
Also, whether it assumes risk scenarios of sufficient extent for cases such as a major delay in batch processing.
- D. Whether the CO reviews assumed scenarios in its contingency plan by, for example, taking into consideration case studies of system troubles, etc. at other financial institutions, clearing organizations, fund clearing organizations, book-entry transfer institutions and trade repositories, and the results of deliberations at the Central Disaster Management Council, etc.
- E. Whether exercises in accordance with the contingency plan involve the entire company and are periodically conducted jointly with outsourced contractors, etc.

F. Whether off-site backup systems, etc. are introduced for important systems whose failure could seriously affect business operations, and that a control environment is in place to address disasters, system troubles, etc. so that normal business operations can be speedily brought back.

**(x) Risk of System Updates, etc.**

A. Whether the CO has developed a control environment for managing the risk of building new systems and updating existing systems (hereinafter referred to as “system updates, etc.”) by ensuring that its officers and employees fully recognize the risk.

B. Whether the CO has established arrangements and procedures for conducting tests. Whether its test plan is suited to the nature of the system development necessitated by the system updates, etc.

C. Whether the CO has established a control environment that enables itself to be proactively involved in the system updates, etc. when this task is outsourced.

D. Whether the CO makes use of third-party evaluation, such as evaluation by a system auditor, when making judgment regarding important matters related to the system updates, etc.

E. Whether the CO has developed a contingency plan for dealing with an unexpected incident.

**(xi) Response to System Troubles**

A. Whether the CO implements appropriate measures to avoid creating unnecessary confusion among investors, participants, etc. when system troubles, etc. occur and performs tasks towards the prompt recovery and operation of alternatives.

Also, whether it has developed a worst-case scenario in preparation for system troubles and is prepared to take necessary measures accordingly.

B. Whether the CO has prepared procedures that also subjects outsourced contractors to reporting system troubles, and has a clearly defined system of command and supervision.

C. Whether the CO is prepared to immediately notify the representative director and other directors when a system trouble that may significantly affect business operations occurs, and report the largest potential risk it poses under the worst-case scenario (for example, if there is a possibility that the failure could gravely affect investors or participants, the reporting persons should not underestimate the risk but immediately report the biggest risk scenario).

In addition, whether it is prepared to launch a task force, have the representative director issue appropriate instructions and orders, and seek resolution of the issue in a



swift manner.

D. Whether the CO, after system troubles, etc. have occurred, analyzes the cause and implements measures based on the analysis to prevent recurrence.

Also, whether it periodically analyzes tendencies of factors that have led to system troubles, etc. and introduces measures to address them.

E. Whether the CO immediately reports system troubles, etc. to the authorities.

### **(3) Supervisory Method and Actions**

#### **(i) At the Time of Problem Recognition**

When supervisory departments have recognized an issue of supervisory concern regarding a CO's control environment for managing information technology risk, through daily supervisory administration, etc., they shall identify and keep track of the status of voluntary improvement made by the CO, by holding in-depth hearings with the CO and the outsourcing contractor and, when necessary, requiring the submission of reports based on Article 156-15 of the FIEA.

When the CO is deemed to have a serious problem from the viewpoint of protecting public interests and investors, the supervisory departments shall take actions such as issuing an order for business improvement, etc., based on Article 156-16 of the FIEA.

#### **(ii) At the Time of System Updates, etc.**

In cases where COs are to perform system updates, etc., they shall be required to submit specific plans for implementing the system updates, etc. and documents regarding the internal control environment for managing the risk associated with the system updates, etc. (including internal audits) and other matters according to their characteristics.

In cases where the system updates, etc. are large in scale, COs shall be required to periodically submit reports based on Article 156-15 of the FIEA until such system updates, etc. are completed.

### **(4) Response to System Troubles**

(i) COs shall be required to notify the authorities of the occurrence of any computer system troubles as soon as they have recognized it, and submit a "Report on Problem Occurrence, etc." (in the format specified in Attached List of Formats 1-1) to the authorities.

After the computer system operation has been restored to normal and the cause of the problem has been identified, they shall be required to report to the authorities again (It should be kept in mind that they shall be required to report to the authorities on the

current state within one month even if the computer system operation has not been restored to normal or the cause of the problem has not been identified within the one-month period.)

(Note) Computer System Trouble Subject to Reporting to the Authorities

Problems that must be reported to the authorities are those which affect systems and equipment (including both hardware and software) used by COs and contractors undertaking business operations outsourced by COs, and which could affect the COs' abilities to identify and keep track of the status of transactions, financial settlements, cash deposits and withdrawals, fund-raising and financial conditions, and undermine the convenience of participants, etc. in other ways.

However, the reporting requirement is not applicable to such system troubles in cases where a backup system has started up and effectively prevented adverse effects.

It should be noted that even if no computer system troubles have occurred, a report must be made in cases where participants or business operations will be affected or are highly likely to be affected, including cases where a CO has received a warning of a cyber attack on its computer system or where it has detected the possibility of such an attack.

(ii) A CO who has reported computer system troubles to the authorities shall be required to submit an additional report based on Article 156-15 of the FIEA when necessary. When the CO is deemed to have a serious problem from the viewpoint of protecting public interests and customers, the authorities shall take actions such as issuing an order for business improvement based on Article 156-16 of the FIEA.

When the CO is deemed to have committed a serious and malicious violation of law, the authorities shall consider necessary actions, including the issuance of an order for business suspension based on Article 156-17 of the FIEA.

### **III-3-5 Procedures to Deal with Participant Default, etc.**

#### **(1) Background and Objectives**

In the event of settlement failure or default of participants, etc. (hereinafter referred to as "default, etc."), the CO needs to promptly take action in order to continue facilitating clearing functions, such as disposing of collateral, procuring financial resources to cover the losses and responding in cases where procurement of additional financial resources becomes necessary.

From this perspective, COs are required to clearly establish procedures to deal with default, etc., including their authority and the participants' obligations. COs also need to

properly verify whether such procedures are actually executable in practice in the event of a participant default, etc.

## **(2) Major Supervisory Viewpoints**

(i) Whether the CO has clearly established procedures in its business rules with respect to the funding of financial resources and other matters in the event of a participant default, etc., in order to enable the continuation of smooth business operations such as the performance of obligations of the CO.

In particular, whether the CO has clearly defined the amount of financial resources required to cover the losses incurred as a result of a participant default, etc. and the order of its use, as well as the authority to carry out additional collections and the method of allocation in cases where losses that cannot be covered by the funding of prefunded financial resources are incurred.

(ii) Also, whether the CO tests periodically, at least once a year, and reviews as necessary, the procedures to deal with a participant default, etc. in collaboration with participants and other parties concerned.

(iii) Whether the CO has developed a manual, etc. to deal with a participant default, etc. and periodically verifies its feasibility with employees involved in the procedures to deal with a participant default, etc., participants and other parties concerned.

(iv) Whether the CO has established clear rules and procedures to settle payment obligations in a timely manner even in the event of individual or combined default, etc. among its participants.

## **(3) Supervisory Method and Actions**

In cases where a problem has been found in the procedures to deal with a participant default, etc., the supervisory departments shall monitor voluntary business improvement made by the CO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-15 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 156-16 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting public interests and investors.

## **III-3-6 Management and Investment of Collateral, etc.**

### **(1) Background and Objectives**

From the viewpoint of protecting customers in the event of the default or the suspension of payment by a participant, it is important that the position and collateral of the participant's customers are managed separately from those of the participant itself. Furthermore, each customer can be protected from the default of the participant and other customers by holding and managing the position and collateral separately on a customer-by-customer basis.

Assuming the situation above, it is important that the collateral provided by the participant, etc. is preserved as an asset with sufficiently high creditworthiness and managed properly by the holding entity, and that the collateral is available for use by the CO promptly at times of emergencies.

For portability (meaning transferring a party's position, etc. to another party), provisions for clear and effective portability procedures are expected to facilitate the transfer of positions, etc. in the event of a participant default, etc. and have the effect of curbing market turmoil under stressed market conditions.

## **(2) Major Supervisory Viewpoints**

(i) Whether the CO has established rules and procedures to enable segregation and portability to hold and transfer customers' positions and collateral related to them in a secure and effective manner in the event of insolvency associated with a participant default, etc.

(ii) Whether the CO has adopted an account structure that enables it readily to identify the positions of a participant's customers and to segregate related collateral.

(Note) Individual account: Method whereby collateral of customers of the CO's participant is managed separately

Omnibus account: Method whereby collateral belonging to all customers of a specific participant is distinguished from the participant's collateral and commingled in a single account

(iii) Whether the CO has established portability rules and procedures for transferring the position/collateral of customers of a defaulting participant to another participant(s).

(iv) Whether the CO has disclosed rules and procedures on the segregation and portability of a participant's customers' positions and related collateral, including whether the participant's customers' collateral is protected either by individual accounts or omnibus accounts.

(v) Whether the CO rigorously selects the entity that will hold the collateral accepted in consideration of said entity's creditworthiness, management arrangements and procedures such as safekeeping procedures, procedures for using collateral at time of

emergency, etc.

(Note) For physical-delivery transactions, supervisory departments shall bear in mind that there are no provisions on the collateral management method in Article 119 of the FIEA, etc. but the purpose of customer protection is fulfilled by Articles 43-2 and 79-20 of the FIEA.

(vi) Whether the CO, in making investments with respect to the deposited collateral, etc., restricts the investment to products with high liquidity or creditworthiness by taking into consideration factors such as the current maturity and nature of products.

(vii) In addition, whether the CO restricts the scale of investment within the scope where prompt cashing is available in times of market stress. Also, whether the CO has made reasonable estimates for assuming that the deposited margin will be retained by the clearing organization for a certain period of time in light of the total amount, past minimum balance and annual payment amount of the deposited margin, etc. and reviews such estimates.

(viii) Whether the CO has developed an investment policy containing the abovementioned details and publicizes it.

### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the arrangements, procedures, etc. for the Management of Collateral, etc., the supervisory departments shall monitor voluntary business improvement made by the CO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-15 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 156-16 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting public interests and investors.

## **III-3-7 Notes concerning Tiered Structure of Participants, etc.**

### **(1) Background and Objectives**

There are tiered participation arrangements in which, when using a CO, a person/entity (indirect participant) uses the CO's system through another person/entity (direct participant). Such tiered participation arrangements enable more participants to access clearing operations as indirect participants through direct participants, while the business structure might become complicated depending on the relationship between direct participants and indirect participants and the nature of the business process, giving rise to

various potential risks. COs need to identify risks inherent in such tiered participation arrangements and establish appropriate arrangements and procedures for managing such risks.

## **(2) Major Supervisory Viewpoints**

- (i) Whether the CO identifies risks involved in tiered participation arrangements and takes measures to manage such risks in its rules, procedures, etc., such as gathering basic information about indirect participation.
- (ii) Whether the CO examines the risks with respect to direct participants with indirect participants' positions that account for a high ratio relative to their financial position identified by gathering information as referred to above or by other means, direct participants, etc. serving as a clearing intermediary for an extremely large number of customers, etc.
- (iii) Whether the CO regularly examines risks to the CO that may arise in the event of the default of an indirect participant, and takes action to mitigate such risks when necessary and appropriate.

## **(3) Supervisory Method and Actions**

In cases where a problem has been found in the arrangements and procedures for managing risks arising from tiered participation arrangements, etc., the supervisory departments shall monitor voluntary business improvement made by the CO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-15 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 156-16 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting public interests and investors.

## **III-3-8 Appropriateness of Disclosure of Information, etc.**

### **(1) Backgrounds and Objectives**

It is important that COs provide sufficient information so that participants and prospective participants can clearly recognize and fully understand the risks and responsibilities arising from their participation in the clearing system.

Furthermore, from the viewpoint of providing sufficient information to participants, etc., it is important that the rights and obligations of participants, etc. and key procedures concerning risks, etc. are clarified and publicly disclosed in business rules and other rules

and procedures.

## **(2) Major Supervisory Viewpoints**

- (i) Whether the CO has formulated clear and comprehensive rules and procedures and disclosed them to participants. Whether the CO publicly discloses key rules, procedures, etc.
- (ii) In the aforementioned rules, procedures, etc., whether the CO clearly describes the rights and obligations of the CO and participants, so that participants can assess the risks they would incur by participating in the CO.
- (iii) Whether the CO clarifies operations performed at a charge and operations performed without charge, and publicly discloses the fee and content of individual services.
- (iv) Whether the CO periodically discloses information based on the “Principles for Financial Market Infrastructures” as well as the “Disclosure framework and Assessment methodology” and “Public quantitative disclosure standards for central counterparties”<sup>(Note)</sup> that supplement the principles.

(Note) CPSS and IOSCO, “Disclosure framework and Assessment methodology” (December 2012)

CPMI and IOSCO, “Public quantitative disclosure standards for central counterparties” (February 2015)

## **(3) Supervisory Method and Actions**

In cases where a problem has been found in the disclosure of major rules, etc. by the CO, the supervisory departments shall monitor voluntary business improvement made by the CO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-15 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 156-16 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting public interests and investors.

### **III-4 Administrative Procedures**

#### **III-4-1 Points to Consider regarding Authorization of Business Rules, etc.**

##### **(1) Background and Objectives**

Business rules prescribe the desirable status of business operations of a CO, as well as basic matters regarding the CO's clearing system such as measures that can be taken by the CO with respect to participants, including requirements for participants, assuming authorization by the authorities.

In light of the above, COs are required to clearly establish rules and procedures, etc. for business rules and clarify their basis and characteristics so that payment and clearing of financial transactions can be performed by participants, participants' customers, etc. in a smooth, continuous and stable manner.

##### **(2) Major Supervisory Viewpoints**

- (i) When preparing and amending business rules, etc. (hereinafter referred to as "amendment, etc."), whether the CO confirms that the clearing system as a whole, including business rules and subordinate rules, etc. is consistent with laws and regulations, etc.
- (ii) Whether the CO discloses and as necessary explains such amendment, etc. to participants, participants' customers, etc. in a clear and easy-to-understand manner at least after receiving authorization by the authorities, or as necessary, before then.
- (iii) When giving such explanation, whether the CO explains the effectiveness and the priority of contracts in the event of a participant default, etc. by summarizing the basis and applicability of laws and regulations pertaining to contracts on clearing, etc.
- (iv) In cases where there is a foreign participant or in cases where assets are held abroad, such as collateral for clearing, whether the CO confirms the risks associated with differences in laws and regulations, such as whether or not the effectiveness of contracts would be undermined in the event of default, etc., including confirming the laws and regulations, etc. of the country concerned.
- (v) When confirming and explaining the above, whether the CO gives consideration to the accuracy of such confirmation and explanation by such means as utilizing outside experts as necessary.
- (vi) In the rules for business rules, etc., whether the CO has clarified the point at which settlement is final in its rules and procedures. Also, whether the CO has clarified at what point unsettled payment, transfer instruction or other obligation becomes



irrevocable by participants.

- (vii) Whether the CO has a structure to properly respond to and manage the following points when the CO adds LG as substitute securities for clearing margins.
  - A. Whether LG issuers are limited to those with high creditworthiness.
  - B. Whether the CO appropriately manages credit concentration risks of financial institutions, including LG issuers.
  - C. Whether the CO appropriately manages liquidity risks with regard to the delivery and receipt of initial margin and variation margin.
  - D. Whether the CO applies appropriate haircuts to the value of LG based on the characteristics of LG
- (viii) Whether the CO confirms that the provisions on the above are consistent with laws and regulations, etc. and explains them to participants, participants' customers, etc.

### **III-4-2 Points to Consider regarding Approval of Subsidiary Business**

#### **(1) Purpose**

If the soundness of a CO is not ensured, there is a risk that not only the stability of the CO's operations, but also the soundness of the financial system as a whole may be undermined through management concerns, etc. of the COs (i.e., systemic risk).

Considering their highly public nature as such, COs must concentrate on financial instruments obligation assumption service and business incidental thereto,<sup>(Note)</sup> and in principle, are not able to conduct any other business, for the purpose of blocking out risks from operations other than their core business (Article 156-6(2) of the FIEA).

On the other hand, based on the view that the provision of services other than their primary business may help improve convenience, stability, etc. of the settlement system as a whole, even if they do not correspond to financial instruments obligation assumption service or business incidental thereto, COs are able to conduct business related to financial instruments obligation assumption service or business of assuming commodity transaction debts, etc. and business incidental thereto that is found to have no risk of hindering their conducting of financial instruments obligation assumption service appropriately and certainly, as related business, by obtaining approval.

(Note) What consists of business incidental to financial instruments obligation assumption service needs to be examined with respect to each individual business, considering that the financial instruments obligation assumption service is aimed at ultimately settling payables and receivables after netting them. For example, the reception of trading data for the assumption of debt, provision of trade matching function concerning transactions

subject to clearing, distribution of settlement instructions, and other such operations that need to be performed in an integrated manner for the smooth execution of the financial instruments obligation assumption service are deemed to correspond to businesses incidental to financial instruments obligation assumption service.

## **(2) Application for Approval**

Upon making an application for approval, the CO shall submit the approval application form prescribed in Article 15(1) of the Cabinet Office Ordinance on Financial Instruments COs, etc. (Attached List of Formats1-2) and the attached documents listed in the items of Article 15(2) of said Ordinance.

## **(3) Approval Screening**

Upon approval screening, it is necessary to determine the appropriateness of approval on a case-by-case basis, in view of such matters as whether there is a risk of hindering the CO from conducting financial instruments obligation assumption service appropriately and certainly. Specifically, approval screening shall be conducted from the following viewpoints.

- (i) Whether there is a high likelihood of causing losses for the CO and affecting its management.
- (ii) Whether the CO has identified the risks to which it will be exposed and established arrangements and procedures for managing such risks properly.
- (iii) Whether there is a risk of undermining confidence in the fairness and impartiality of the clearing operations or undermining the social credibility as a CO.
- (iv) Whether the workload hinders the appropriate operation of the financial instruments obligation assumption service.
- (v) Whether the business, in light of its content and characteristics, helps the smooth operation of the financial instruments obligation assumption service. Whether the business helps facilitate the circulation of securities, etc. through increasing in the convenience for participants, participants' customers, etc.

## **(4) Supervisory Method and Actions after Granting Approval**

COs are important social infrastructures that ensure speedy and reliable means of settlement, and authorities are required to conduct monitoring on an ongoing basis so that the sound and appropriate operation of their primary business is not hindered due to other business operations, say, as a result of confidence in COs being undermined.

In cases where other business conducted by a CO is hindering or has the risk of

hindering the sound and appropriate operation of its primary business, the supervisory departments shall monitor voluntary business improvement made by the CO, by holding an in-depth hearing and, when necessary, requiring the submission of a report based on Article 156-15 of the FIEA.

Furthermore, the supervisory departments shall consider taking actions, such as issuing an order for business improvement under the provision of Article 156-16 of the FIEA) when it is deemed necessary and appropriate to do so from the viewpoint of protecting the public interests and investors.

#### **IV. Supervisory Viewpoints and Procedures (Fund Clearing Organizations)**

##### **IV-1 Governance / Business Administration**

###### **IV-1-1 Governance System**

###### **(1) Background and Objectives**

More appropriate risk management, etc. than ever is required for FCOs as their operations are becoming increasingly complex. Under these circumstances, there shall be effective disciplines for management and proper governance in FCOs, in order to ensure appropriate business operations and sound management of FCOs, and in turn, financial system stability.

Effective functioning of governance presumes that the components of the organization are fulfilling their primary roles. Specifically, it is important that, for example, organs such as the board of directors and the board of auditors are able to check management, and checks and balances among divisions are functioning properly, as is the internal audit section. It is also necessary for directors, etc. (directors, auditors, accounting advisors) and employees in all positions to understand their respective roles and be fully involved in the process.

(Note) In the case of FCOs that have established nominating committees, it is necessary to examine whether the board of directors, nominating committees, executive officers, etc. are properly exercising their respective authority appropriately. In addition, in the case of FCOs that have established an audit and supervisory committee, it is necessary to examine whether the board of directors and audit and supervisory committee, etc. are properly exercising their respective authority. In this case, examination should be conducted with due consideration of the actual status of management based on the purpose of these Guidelines.

## **(2) Major Supervisory Viewpoints**

### **[Representative Director]**

- (i) Whether the representative director considers compliance as one of the important management issues and takes the initiative in building a control environment for compliance.
- (ii) Whether the representative director fully recognizes that disregarding the risk management division may have a serious impact on corporate earnings and attaches importance to the said division.

### **[Directors/Board of Directors]**

- (i) Whether directors check and prevent autocratic management by the representative director and other officers who are responsible for business execution, and are actively involved in the board of directors' decision-making and checking process concerning business execution.
- (ii) In cases where outside directors are appointed, whether they recognize their own significance from the viewpoint of ensuring objectivity in the decision-making of management, etc. and proactively participate in the meetings of the board of directors. In cases where proposals for the appointment of outside directors are to be determined, whether the outside directors' personal relationships and equity relationships with the FCO and other interests are verified and their independence, aptitude, etc. are carefully examined, in consideration of the roles they are expected to fulfill. Whether some kind of framework has been established so that outside directors would make appropriate judgments at the meetings of the board of directors; for example, whether information is provided on an ongoing basis.
- (iii) Whether the board of directors takes measures to objectively ensure the appropriateness and fairness of, for example, important management decisions and management judgments related to compliance, credit risk management, etc. such as utilizing the advice of outside experts and discretionary committees whose members consist of outside experts as necessary when making such decisions and judgments. In particular, whether the board of directors takes measures to appropriately reflect the legitimate interests of its direct and indirect participants and other relevant stakeholders on design, rules, overall strategy, and major decisions.
- (iv) Whether the board of directors has specified a management policy based on the overall vision of the desirable status of the FCO. Whether it has established management plans in line with the management policy and communicated the plans throughout the

- organization. Whether it regularly reviews and revises the progress status thereof.
- (v) Whether directors and the board of directors are sincerely leading efforts in compliance and are properly demonstrating the board's functions to establish an organization-wide internal control environment.
  - (vi) Whether the board of directors fully recognizes that disregarding the risk management division may have a serious impact on corporate earnings, and attaches importance to the said division. In particular, whether the director in charge has in-depth knowledge and understanding concerning the methods of measuring, monitoring and managing risks, in addition to an understanding of where risks reside and what kind of risks they are.
  - (vii) Whether the board of directors has set up a policy for managing risks based on strategic objectives and communicated it throughout the organization. Whether it reviews the risk management policy on a periodic or as-needed basis. In addition, whether the board of directors makes use of risk-related information in the execution of business and the development of risk management systems by, for example, making necessary decisions based on the status of risks reported periodically.

**[Auditors/Board of Auditors]**

- (i) Whether the independence of the auditors and the board of auditors is ensured in accordance with the purpose of the board of auditors system.
- (ii) Whether the auditors and the board of auditors properly exercise the broad authority granted thereto and conduct audits of business operations in addition to audits of accounting affairs.
- (iii) Whether individual auditors recognize the importance of their own independence within the board of auditors and actively take the initiative to conduct audits.
- (iv) Whether the auditors and the board of auditors strive to ensure the effectiveness of their audits by, for example, receiving reports on the results of external audits, depending on the contents thereof.

**[Internal Audit Section]**

- (i) Whether the internal audit section is independent from divisions subject to audit so as to fully check the actions thereof, has the control environment and ability to collect important information on their operational status, etc. in a timely manner, and is sufficiently staffed and equipped to conduct effective internal audits that are accurately adapted to the environment surrounding the FCO and its operational status.
- (ii) Whether the internal audit section formulates efficient and effective internal audit plans that give consideration to frequency and depth according to the type and magnitude of

risks based on its understanding of the status of risk management, etc. by divisions subject to audits, properly reviews the plans depending on the situation, and conducts efficient and effective internal audits based on the internal audit plans.

- (iii) Whether the internal audit section reports important issues pointed out in internal audits without any delay to the representative director and the board of directors. Whether the internal audit section has accurately identified the status of improvements made on the issues pointed out.

#### **[Use of External Audits]**

- (i) Whether external audits are effectively utilized, with sufficient understanding that effective external audits are indispensable for ensuring sound and appropriate business operations of FCOs.
- (ii) Whether external audits are examined periodically as to whether they are effectively functioning, and appropriate measures are taken with respect to the external audit results, etc.
- (iii) Whether such matters as the number of consecutive years of service by a certified public accountant involved are handled properly.

### **(3) Supervisory Method and Actions**

Supervisory departments shall examine the status of governance through the following hearings and daily supervisory administrative processes.

#### **(i) Comprehensive Hearings (See II-1-1 (1))**

Supervisory departments shall hold hearings regarding FCOs' management challenges, strategies and the status of risk management and governance, among other matters. In addition, senior supervisory departments shall directly hold hearings with top managers of FCOs as necessary.

#### **(ii) Examination of Governance through Daily Supervisory Administrative Processes**

Supervisory departments shall examine the effectiveness of governance not only through the hearings described above but also through daily supervisory administrative processes, such as follow-up on reports on business improvements made on matters pointed out in inspections.

#### **(iii) Recording of Monitoring Results**

Supervisory departments shall compile and store records on matters of particular note based on the results of monitoring conducted through procedures described above, and make effective use thereof in future supervisory administrative processes.

#### **(iv) Supervisory Method and Actions**

In cases where doubt has arisen about the effectiveness of an FCO's governance, the supervisory departments shall monitor voluntary business improvement made by the FCO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 80(1) of the PSA.

Furthermore, the supervisory departments shall take actions such as issuing an order for business improvement based on Article 81 of the PSA, when it is deemed necessary to do so from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

#### **IV-1-2 Officers of Fund Clearing Organizations**

##### **(1) Major Supervisory Viewpoints**

From the viewpoint of maintaining the public nature of fund clearing operations, supervisory departments shall pay attention to the following points when examining the decision-making process regarding proposals for the appointment of officers of the FCO, among others.

- (i) The officer shall neither meet any of the ineligibility criteria (Article 66(2)(iv)(a) to (e) of the PSA) nor have met any of them at the time when the FCO obtained a license.
- (ii) The officer shall neither have violated laws and regulations regarding fund clearing operations or business related thereto nor have breached any administrative actions taken based on laws and regulations.
- (iii) The officer shall not have engaged in an illegal or markedly inappropriate act regarding fund clearing operations under particularly grave circumstances.

##### **(2) Supervisory Method and Actions**

Supervisory departments shall consider taking actions, such as ordering the dismissal of an officer of an FCO under the provisions of Article 66(2)(iv)(a) to (e) of the PSA when said officer: (i) meets any criteria specified in Article 67(3) or Article 82(2) of the PSA, or is found to have already met such criteria at the time when the FCO obtained license; (ii) is found to have become an officer of the FCO by fraudulent means; or (iii) violates or is found to have violated laws and regulations or administrative actions taken based on laws and regulations.

In addition, they shall hold an in-depth hearing regarding the decision-making process concerning the proposal for the appointment of the said officer or committee member and, when necessary, require the submission of a report based on Article 80(1) of the PSA.

Furthermore, supervisory departments shall consider taking actions, such as issuing an order for business improvement (Article 81 of the PSA), if the FCO's control environment for governance is deemed to have a serious problem and the action is deemed to be necessary, from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

#### **IV-1-3 Staffing**

##### **(1) Major Supervisory Viewpoints**

Supervisory departments shall examine whether FCOs are adequately staffed to properly and reliably conduct fund clearing operations in light of the following requirements regarding FCOs' officers and employees.

- (i) Whether the FCOs have secured officers and employees who understand the viewpoints regarding governance that are specified under the PSA and other relevant regulations, as well as these Guidelines, and who have the knowledge and experience necessary for conducting governance as well as sufficient knowledge and experience concerning the control environment for compliance and risk management required to properly and reliably execute the fund clearing operations.
- (ii) Whether officers or employees are current or former members of organized crime groups or have a close relationship with organized crime groups.
- (iii) Whether officers or employees have the experience of being sentenced to a fine (including similar punishments imposed under foreign laws and regulations equivalent thereto) for violation of the PSA or other domestic financial laws and regulations or foreign laws and regulations equivalent thereto.
- (iv) Whether officers or employees have the experience of being sentenced to a fine (including similar punishments imposed under foreign laws and regulations equivalent thereto) for violation of the Act on Prevention of Unjust Acts by Organized Crime Group Members (excluding the provisions of Article 32-3(7) and Article 32-11(1) of said Act) or other foreign laws and regulations equivalent thereto, or for committing a crime prescribed under the Penal Code or under the Act on Punishment of Physical Violence and Others.
- (v) Whether officers or employees have the experience of being sentenced to imprisonment with work or more severe punishment (including similar punishments imposed under foreign laws or regulations equivalent thereto). In particular, whether officers or employees have been accused of committing crimes specified under Articles 246 to 250 of the Penal Code (fraud, fraud using computers, breach of trust, quasi fraud and



extortion as well as attempts at these crimes).

**(2) Supervisory Method and Actions**

The requirements specified in (i) to (v) above are part of a comprehensive set of elements that should be taken into consideration when supervisory departments examine whether an FCO is adequately staffed to properly and reliably conduct fund clearing operations. Even if an officer or an employee is deemed to not meet the requirements, it should not automatically lead to the conclusion that the FCO is not adequately staffed. The important thing is, first and foremost, that FCOs strive to ensure on their own responsibility that they are adequately staffed, in light of those requirements and other elements.

However, supervisory departments shall hold in-depth hearings regarding the FCO's awareness of such staffing and the decision-making process concerning the proposed appointments of officers and employees, in cases where an FCO is deemed to have failed to take those elements into consideration sufficiently in the said decision-making process, and where it is deemed to be necessary to hold such hearings in relation to the business operations of the FCO from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner. In addition, they shall require the submission of reports under the provision of Article 80(1) of the PSA when necessary.

Supervisory departments shall consider taking actions, such as issuing an order for business improvement under Article 81 of the PSA, in cases where the FCO's control environment for governance is deemed to have a serious problem as a result of the examination of the submitted report, and where the action is deemed to be necessary from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

## **IV-2 Financial Soundness**

### **IV-2-1 Adequacy of Capital**

#### **(1) Background and Objectives**

In order for FCOs to gain participants' and others' confidence and to operate their business continuously and stably, it is important for FCOs to retain a sufficient financial basis according to the characteristics of management as well as to establish appropriate arrangements and procedures for managing credit risks, liquidity risks and other such risks.

Accordingly, FCOs should hold enough liquid assets to withstand any losses that may be incurred in the event that various risks are actualized.

FCOs also need to have a process for evaluating their capital adequacy in the context of their risk profiles, and implement appropriate measures for maintaining a sufficient level of capital.

#### **(2) Major Supervisory Viewpoints**

##### **[Directors/Board of Directors]**

- (i) Whether the directors have a general understanding of the nature and level of the risks taken by the FCO as well as the relationship between risk and the appropriate level of capital.
- (ii) Whether the directors and the board of directors understand that, in order to achieve their strategic objectives, a capital plan, which is consistent with them, is an essential component, and whether they have formulated an appropriate capital plan according to the management issues of the FCO.
- (iii) Whether the directors have been sufficiently involved in formulating the aforementioned capital plan, and are adopting a process for evaluating capital adequacy and implementing appropriate measures for maintaining a sufficient level of capital.

##### **[Capital Adequacy]**

- (i) Upon formulating the aforementioned capital plan, whether the FCO evaluates the adequacy of capital relative to the risks measured in comprehensive risk management conducted in consideration of changes in the business environment, etc.
- (ii) As for the amount of assets (e.g. the amount of net assets) to be held to prepare against business risks, which should not include financial sources procured for the purpose of preparing against credit risks and liquidity risks incurred in participant default, whether the FCO has secured at least six months worth of operating expenditures, and has

examined the sufficiency of the level of such amount in consideration of ensuring its business continuity.

- (iii) Whether the FCO properly examines equity capital, for example, as to whether the equity capital consists primarily of cash and cash equivalents, etc. and can thus be easily liquidated in a stress scenario.
- (iv) Whether the FCO has a feasible plan to raise additional capital if the level of capital approaches or falls below levels that would make its business continuity uncertain.

## **IV-2-2 Comprehensive Risk Management Framework**

### **(1) Background and Objectives**

FCOs that intensively undertake the clearing of claims and liabilities related to exchange transactions conducted between banks, etc. face a wide range of risks, including not only risks arising directly from the burden of liabilities, etc. based on exchange transactions, such as credit risks and liquidity risks, but also information technology risks and operational risks. FCOs are required to confirm whether such risks would affect the soundness of their financial condition, etc. and establish appropriate arrangements and procedures for risk management.

Individual FCOs are expected to establish frameworks for high-precision risk management that suits their own circumstances.

Also, in cases where a financial institution, etc. that is a clearing participant provides money settlement and liquidity supply functions for an FCO, it is important that the FCO are aware that risks with such financial institution, etc. will not be limited to credit risks and that FCOs needs to identify the risks with such financial institutions in a comprehensive manner.

### **(2) Major Supervisory Viewpoints**

- (i) Whether the risk management division has sufficient authority, independence, resources, and access to the board in order to conduct effective risk management. For example, whether the reporting lines for risk management are clear and separate from those for other operations of the FCO, so that the matters can be directly reported to the board of directors by the authority of the risk management division.
- (ii) Whether the FCO has revealed and identified all risks in order to grasp diverse risks in a comprehensive manner, and if possible, has properly determined risk categories to place them under quantitative risk management.
- (iii) Whether the FCO reviews the scope of quantification and accuracy to improve them as

necessary. For example, whether the FCO reviews the importance, correlation, etc. of different types of risks to ensure appropriateness.

- (iv) Whether the board of directors has clearly set up a policy for managing risks based on strategic objectives in accordance with the management policy of the FCO as a whole, and examines the policy periodically, at least annually, and revises it as necessary. In addition, whether the board of directors takes appropriate measures to make the risk management policy widely known within the organization.
- (v) Whether the board of directors makes use of risk-related information in the execution of business and the development of risk management systems by, for example, making necessary decisions based on risk status reports received periodically.
- (vi) In cases where the money settlement functions are entrusted to a financial institution other than the BOJ, whether the FCO identifies the creditworthiness, capital, liquid assets and other conditions of such money-settling financial institution in a timely manner, and examines and controls risk management in a comprehensive manner in view of whether credit and liquidity risks are over-concentrated in such money-settling financial institution.

#### **IV-2-3 Credit Risk Management**

##### **(1) Background and Objectives**

FCOs bear the risk of incurring losses from the deterioration in the financial position, failure of settlement, etc. on the part of the clearing participants, settlement banks and other parties to transactions in the course of payment and clearing.

Especially in the event of a participant default, etc., there is a possibility that rapid credit crunch, etc. among participants might give rise to serious turmoil in fund clearing operations.

For this reason, FCOs are required to manage credit exposures to participants with precision, combine the management of collateral and other systems and techniques, limit potential losses that may arise from the nonperformance of obligation, etc. by participants and minimize their own losses as well as the losses of other participants.

##### **(2) Major Supervisory Viewpoints**

- (i) Whether the FCO has established a policy to manage credit risks that arise in the course of clearing operations conducted such as credit exposures to participants.
- (ii) Whether the FCO grasps its status of compliance with policies to identify the source of credit risks, periodically measure the amount of credit risks and manage credit risks, and

as necessary, takes measures such as reducing the amount of risks.

- (iii) Whether the FCO takes measures to ensure the appropriateness, etc. of its credit risk management policy, such as utilizing participants and other outside experts as necessary, when formulating such policy. Whether the FCO examines the appropriateness, etc. of the policy periodically, at least annually, according to changes in the external environment, etc. and revises it as necessary.
- (iv) Whether the FCO covers credit exposures to participants with a high degree of confidence using collateral or equivalent prefunded financial resources. Specifically, whether the FCO secures necessary prefunded financial resources by such means as implementing the collateral system referred to in IV-2-5.

#### **IV-2-4 Liquidity Risk Management**

##### **(1) Background and Objectives**

When a counterparty to a transaction cannot make the settlement by the due date, even though the counterparty may perform its obligation at some point in the future, the FCO will incur a loss due to the nonperformance of such obligation (liquidity risk).

In such cases, the FCO has to complete the settlement with its own liquid assets to cover the shortfall in funds arising from the failure of such obligation with its own liquid assets; FCOs are thus required to manage liquidity risks with precision by such means as identifying liquidity risks and securing liquid assets commensurate with such risks.

##### **(2) Major Supervisory Viewpoints**

- (i) Whether the FCO has established a policy to manage liquidity risks that arise in the course of clearing operations conducted. Whether the FCO has effective operational and analytical tools to monitor its settlement and funding flows on an ongoing and timely basis.
- (ii) Whether the liquidity resources maintained cover the stress scenarios, in consideration of extreme but plausible market conditions, such as the default of two participants (on a non-consolidated basis)<sup>(Note 1)</sup> that require the most liquid resources. Whether the liquidity resources cover at least the default of one participant (on a consolidated basis)<sup>(Note 2)</sup> that require the most liquid resources.

(Note 1) This refers to the amount calculated without including companies associated with such participant (meaning the subsidiaries and affiliates of said participant, parent of said participant, subsidiaries of said parent and affiliates of said parent).

(Note 2) This refers to the amount calculated by including companies associated with such participant.

- (iii) Whether the FCO limits liquid assets to deposits with the BOJ and financial institutions, commitment lines or others subject to a prearranged funding arrangement which can be immediately used and cashed in the event of an emergency.
- (iv) Whether the FCO sufficiently confirms that the provider of liquid assets has the capacity to provide liquidity based on the prearranged arrangement, such as by having established arrangements and procedures to manage its own liquidity risk with precision.
- (v) In cases where the FCO has access to the BOJ's accounts, payment services and securities settlement services, if practical, whether the FCO uses such services to enhance its management of liquidity risks.
- (vi) Whether the FCO regularly tests the sufficiency of the aforementioned liquid financial resources through rigorous stress testing, while taking into consideration the following points.
  - A. In conducting stress testing, whether there is a spectrum which takes into consideration a variety of extreme but plausible market conditions, such as default of multiple participants, and pressure in markets in the event of participant default.
  - B. Whether the FCO conducts stress testing and back testing on a daily basis using predetermined scenarios, models, parameters, etc. according to its risk management policy. Whether the FCO has formulated clear procedures to report the test results to the appropriate decision makers in the FCO, evaluate the sufficiency of financial resources, and secure additional resources as necessary.
  - C. Whether the FCO analyzes the appropriateness of the adopted scenarios, models, parameters, etc. in detail on at least a monthly basis. Whether the FCO analyzes the scenarios, etc. more frequently if it is deemed necessary to do so when, for example, liquidity decreases, or the size or concentration of positions held by participants increases significantly.
  - D. Whether the FCO performs a full validation of its risk-management model overall and revises the model as necessary at least annually, in conjunction with the examination of its policy to manage the aforementioned risks.

#### **IV-2-5 Collateral System**

##### **(1) Background and Objectives**

Collateral is significant in that it not only reduces the credit risks borne by FCOs by protecting their credit exposures but also gives participants the incentive to manage risks.

On the other hand, the liquidation value of collateral varies with market conditions, so under stressed market conditions such as in the event of participant default, market price and liquidity may rapidly fall.

For this reason, FCOs need to apply prudent haircuts to the value of the collateral so that the liquidation value of the collateral under stressed market conditions would be equal to or greater than the amount subject to protection, and establish arrangements and procedures so that the collateral can actually be disposed of under stressed market conditions.

## **(2) Major Supervisory Viewpoints**

- (i) Whether the FCO generally limits the assets it accepts as collateral to those with low credit, liquidity, and market risks.
- (ii) Whether the FCO develops haircuts by establishing prudent collateral valuation practices. Whether the haircuts are regularly tested and take into account stressed market conditions.
- (iii) In order to reduce the need for procyclical adjustments, whether the FCO establishes stable and conservative haircuts that are calibrated to include periods of stressed market conditions, to the extent practicable and prudent.
- (iv) Whether the FCO takes measures to avoid concentrated holdings of certain assets as collateral.
- (v) Whether the FCO that accepts foreign collateral mitigates the risks associated with its use and ensures that the collateral can be used in a timely manner.

## **IV-2-6 Supervisory Method and Actions**

In cases where a problem has been found in the soundness of the financial condition or the status of the risk management arrangements and procedures of an FCO, the supervisory departments shall monitor voluntary business improvement made by the FCO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 80(1) of the PSA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 81 of the PSA when it is deemed necessary to do so from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

## **IV-3 Operational Appropriateness**

### **IV-3-1 Compliance**

#### **IV-3-1-1 Measures for Ensuring Compliance**

##### **(1) Notes Regarding Policies, Procedures, etc. Pertaining to Compliance**

- (i) Whether the FCO regards compliance as one of the most important issues for management, and whether it has formulated a basic policy concerning the implementation of compliance, as well as a detailed implementation plan (compliance program) and a code of conduct (ethics code, compliance manual), etc.
- (ii) Whether the FCO has clearly established the authority and responsibility of the chief compliance officer, and whether there is a system in place for his/her function to be fully exercised.
- (iii) Whether the FCO has established a system for communicating and reporting compliance-related information appropriately among the management team, the divisions in charge of the clearing operations, and the compliance division, chief compliance officer or other person in charge.

##### **(2) Notes Regarding the Whistle-blowing System**

- (i) Whether the FCO has clearly designated the division in charge of the whistle-blowing system and established specific procedures for handling internal allegations, so as to ensure that they are processed and a response is made in a prompt and appropriate manner.
- (ii) Whether the FCO has developed a system wherein information on the content of internal allegations can be shared within a necessary and appropriate scope.
- (iii) Whether the FCO makes sure to properly follow up on how internal allegations are being handled.
- (iv) Whether the FCO accurately and appropriately records and stores the details of internal allegations and the results of investigations thereof, and whether it makes full use of this information such as to improve its operational control system and to formulate measures for preventing a recurrence.

#### **IV-3-1-2 Fair Participation Requirements, etc.**

##### **(1) Background and Objectives**



Given the role of FCOs, which is to contribute to the stable and efficient business operations of market participants by intensively executing processes, etc. in financial transactions, FCOs' services should be fair and open to participants, other FCOs, etc.

At the same time, FCOs are required to establish reasonable risk-related participation requirements and manage the risks of participants to which FCOs are exposed, in order to ensure their own financial soundness and provide clearing services in a stable manner.

## **(2) Major Supervisory Viewpoints**

- (i) Whether the FCO has established reasonable risk-related participation requirements for participants.
- (ii) Whether the FCO examines whether such participation requirements are fair or not from the viewpoint of providing fund clearing services in a stable manner, etc. and releases the participation requirements to the public in consideration of such examination.
- (iii) Whether the FCO abuses its position in such circumstances as using information received from fund clearing operations in other services and concluding contracts on services related to fund clearing operations.
- (iv) Whether the FCO monitors compliance with its participation requirements on an ongoing basis, such as by receiving reports on the financial position, etc. from participants in a timely manner. Whether the FCO has clearly defined and publicly disclosed procedures for facilitating the suspension and exit of fund clearing participants who no longer meet the participation requirements.

## **(3) Supervisory Method and Actions**

In cases where a problem has been found in the participation requirements or compliance monitoring, the supervisory departments shall monitor voluntary business improvement made by the FCO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 80(1) of the PSA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 81 of the PSA when it is deemed necessary and appropriate to do so from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

### **IV-3-1-3 Prevention of Damage that May be Inflicted by Anti-Social Forces**

## **(1) Background and Objectives**

Eliminating anti-social forces from society is a task critical to ensuring the order and safety of society, so it is necessary and important to promote efforts to ban any relations with anti-social forces from the viewpoint of fulfilling social responsibility. In particular, as FCOs are highly public in nature and play an important economic role, they need to exclude anti-social forces from financial instruments markets in order to prevent damage from being inflicted not only on itself and their officers and employees but also on various stakeholders who participate in financial instruments markets.

Needless to say, if FCOs are to retain public confidence and maintain the soundness and appropriateness of their business operations, it is essential that they deal with anti-social forces in accordance with laws and regulations without bowing to pressure from them. Therefore, FCOs must strive, on a daily basis, to develop a control environment for banning any relations with anti-social forces in accordance with the purpose of the “Guideline for How Companies Prevent Damage from Anti-Social Forces” (agreed upon at a meeting on June 19, 2007, of cabinet ministers responsible for anti-crime measures).

In particular, anti-social forces have become increasingly sophisticated in their efforts to obtain funds, disguising their dealings as legitimate economic transactions through the use of affiliated companies in order to develop business relations with ordinary companies. In some cases, the relations thus developed eventually lead to problems. In order to deal with such cases properly, the management teams of FCOs need to take a resolute stance and implement specific countermeasures.

It should be noted that if an FCO delays specific actions to resolve a problem involving anti-social forces on the grounds that unexpected situations, such as the safety of officers and employees being threatened, could otherwise arise, the delay could increase the extent of the damage that may be ultimately inflicted on the FCO.

(Reference) “Guideline for How Companies Prevent Damage from Anti-Social Forces”  
(agreed upon at a meeting on June 19, 2007, of cabinet ministers responsible  
for anti-crime measures)

### **(i) Basic Principles on Prevention of Damage that May be Inflicted by Anti-social Forces**

- Institutional response
- Cooperation with external expert organizations
- Ban on any relations, including transactions, with anti-social forces
- Legal responses, both civil and criminal, in the event of an emergency
- Prohibition of engagement in secret transactions with and provision of funds to anti-social forces

## **(ii) Identification of Anti-social Forces**

In judging whether specific groups or individuals constitute “anti-social forces,” which are defined as groups or individuals that pursue economic profits through the use of violence, threats and fraud, it is necessary not only to pay attention to whether they fit the definition in terms of their affiliation, such as whether they constitute or belong to *boryokudan* crime syndicates, *boryokudan* affiliated companies, *sokaiya* racketeer groups, groups engaging in criminal activities under the pretext of conducting social campaigns or political activities and crime groups specialized in intellectual crimes, but also to whether they fit the definition in terms of the nature of their conduct, such as whether they are making unreasonable demands that go beyond the limits of legal liability. (Refer to the “Key Points of Measures against Organized Crime,” a directive issued in the name of the Deputy Commissioner-General of the National Police Agency on December 22, 2011.)

## **(2) Major Supervisory Viewpoints**

An FCO should not have any relations with anti-social forces and, in cases where it has established a relationship with an anti-social force unwittingly, supervisors, while also giving consideration to the characteristics of specific transactions, shall pay attention to such as the following points in order to examine its control environment for banning any relations with anti-social forces as soon as possible after the counterparty has been found to be an anti-social force and its control environment for dealing with unreasonable demands by anti-social forces appropriately.

### **(i) Institutional response**

In light of the need and importance of an action to ban any relationship with anti-social forces organically, whether the responsibility of responding to the situation is not left solely to the relevant individuals or divisions but the management including directors are appropriately involved, and there is a policy for the entire organization to respond. In addition, whether there is a policy calling for the corporate group as a whole, not just the involved FCO alone, to take on an effort to prevent any relationship with anti-social forces. Furthermore, whether the FCO is also making efforts to eliminate anti-social forces when conducting transactions including the provision of financial services under business alliance with other companies outside of the corporate group.

### **(ii) Developing of a Centralized Control Environment through anti-social forces response division**

Whether the FCO has established an anti-social forces response division so as to develop a centralized control environment for preventing anti-social forces from inflicting damage, and whether this division is properly functioning.

In particular, whether the FCO pays sufficient attention to the following points in developing the centralized control environment.

- A. Whether the anti-social forces response division is actively collecting and analyzing information on anti-social forces and has developed a database to manage it (i.e., addition, deletion or change of information in the database). Further, whether the division is making efforts to share information within the group in the process of collecting and analyzing such information. Whether the anti-social forces response division has a system to appropriately take advantage of such information for screening the counterparties of transactions and evaluating the attributes of shareholders of the FCO.
- B. Whether the FCO makes sure to maintain the effectiveness of measures to ban any relations with anti-social forces by, for example, having the anti-social forces response division develop a manual for dealing with anti-social forces, provide on-going training, foster cooperative relationships with external expert organizations such as the police, the National Center for the Elimination of Boryokudan and lawyers, on an ongoing basis. In particular, whether the FCO is prepared to report to the police immediately when it faces the imminent prospect of being threatened or becoming the target of an act of violence, by maintaining close communications with the police on a daily basis so as to develop a systematic reporting system and build a relationship that facilitates cooperation in the event of a problem.
- C. Whether the FCO has a structure in which relevant information is appropriately conveyed to the anti-social forces response division for consultation when transactions with anti-social forces are found or such forces have made unreasonable demands. Further, whether the anti-social forces response division has a structure to appropriately report relevant information to the management. In addition, whether the anti-social forces response division has a structure to ensure the safety of individuals encountering anti-social forces in person and to support the divisions in dealing with them.

**(iii) Execution of Appropriate Prior Screening**

Whether the FCO bans allowing anti-social forces to become a participant or counterparty to a transaction by conducting appropriate advance screening using information on such forces in order to prevent transactions with anti-social forces, and makes sure provisions regarding the exclusion of “boryokudan” crime syndicates are

introduced in all contracts and terms of transactions.

**(iv) Execution of Appropriate Follow-up Review**

Whether, for the purpose of making sure any relationships with anti-social forces are eliminated, there is a structure to conduct an appropriate follow-up review on existing claims and contracts.

**(v) Measures to Terminate Transactions with Anti-Social Forces**

A. Whether the FCO has a system under which information confirming the existence of a transaction with anti-social forces is appropriately reported to the management, including directors, etc., via the anti-social forces response division, and responds to the situation under appropriate directions and involvement by the management.

B. Whether the FCO regularly communicates with external expert organizations, including the police, the National Center for the Elimination of Boryokudan, lawyers and so forth, and promotes efforts to eliminate any transactions with anti-social forces.

C. Whether the FCO, when it has learned through a follow-up review after initiating a transaction that the counterparty is a member of an anti-social force, takes measures to prevent the provision of benefits to anti-social forces, such as seeking collection to the extent possible.

D. Whether the FCO has a structure to prevent providing funds or engaging in inappropriate or unusual transactions for whatever reason if the counterparty has been found to be an anti-social force.

**(vi) Dealing with Unreasonable Demands by Anti-Social Forces**

A. Whether the FCO has a system under which the information that anti-social forces have made unreasonable demands is immediately reported to the management including directors, etc. via the anti-social forces response division and responds to the situation under appropriate directions and involvement by the management.

B. Whether the FCO actively consults external expert organizations such as the police, the National Center for the Elimination of Boryokudan, and lawyers, when anti-social forces make unreasonable demands, and responds to such unreasonable demands based on guidelines set by the National Center for the Elimination of Boryokudan and other organizations. In particular, whether the FCO has a structure to report to the police immediately when there is an imminent prospect of a threat being made or an act of violence being committed.

C. Whether the FCO has, in response to unreasonable demands by anti-social forces, a policy to take every possible civil legal action and to avoid hesitating to seek the initiation of a criminal legal action by proactively reporting damage to the authorities.

D. Whether the FCO ensures that the division in charge of handling problematic conduct

promptly conducts a fact-finding investigation upon request from the anti-social forces response division, in cases where the unreasonable demand from anti-social forces is based on problematic conduct related to business activity or involving an officer or employee.

**(vii) Management of Shareholder Information**

Whether the FCO manages shareholder information properly, through means such as checking the transaction status of its own shares and examining information regarding the attributes of its shareholders.

**(3) Supervisory Method and Actions**

When supervisory departments have recognized an issue of supervisory concern regarding an FCO's control environment for banning any relations with anti-social forces, through inspection and daily supervisory administration, they shall identify and keep track of the status of voluntary improvement made by the FCO by holding in-depth hearings and, when necessary, requiring the submission of reports based on Article 80(1) of the PSA. When the FCO is deemed to have a serious problem from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner because its internal control environment is extremely fragile, as shown by, for example, a failure to take appropriate steps toward dissolving relations with anti-social forces despite recognizing the provision of funds thereto and the presence of inappropriate business relations therewith, supervisory departments shall take actions such as issuing an order for business improvement based on Article 81 of the PSA.

**IV-3-2 Business Continuity Management (BCM)**

**(1) Background and Objectives**

FCOs assume liabilities of financial instruments intensively and settle transactions in large amounts. They are required to take such actions as formulating an appropriate business continuity plan (BCP) in order to recover their operations as soon as possible and continue their operations even in the event of an emergency, e.g., acts of terrorism, large-scale disasters.

**(2) Major Supervisory Viewpoints**

(i) Whether the FCO recognizes what constitutes an emergency and is striving as much as possible to prevent or guard against any emergency by, for example, conducting inspections and anti-crisis practices periodically in normal times.

- (ii) Whether the FCO formulates emergency response policies, etc., including a BCP, to recover their operations as soon as possible and continue their operations even in the event of an emergency, and periodically reviews them. In particular, whether the FCO clarifies its decision-making system in crises.
- (iii) Whether the board of directors clearly defines the roles and responsibilities for addressing an emergency and endorses the CO's operational risk-management framework in the case of formulating and significantly changing the emergency response policies, etc.
- (iv) Whether the BCP, etc. aims to resume the operation of the indispensable information system within two hours from system halt (to resume processing with a backup system immediately) and to complete settlement on the same day on which the fault occurred.
- (v) Whether the FCO has developed a control environment for promptly making a report to Banks Division I, Supervisory Bureau of the FSA and making relevant organizations within the FCO work closely with each other if an emergency has arisen or if the possibility of an emergency has been recognized.
- (vi) Whether the FCO has established a backup center while taking geographic factors into account as a safety measure to prepare against emergencies. Whether the FCO backs up business data in a timely manner and periodically conducts drills such as switching over to the backup center.
- (vii) Whether the FCO has considered measures assuming the possibility of electricity supply, communication lines, public transport and other social infrastructures coming to a halt.

### **(3) Supervisory Method and Actions**

When supervisory departments have recognized an issue of supervisory concern regarding an FCO's control environment for crisis management, through daily supervisory administration, etc., they shall identify and keep track of the status of voluntary improvement made by the FCO by holding in-depth hearings and, when necessary, requiring the submission of reports based on Article 80(1) of the PSA.

When supervisory departments have recognized the occurrence of an emergency or the likelihood of an emergency occurring, they shall hold hearings periodically and check the situation first-hand so that they can identify and keep track of how the relevant FCO is responding to the emergency, including whether the response (status of the development of a control environment for crisis management, securement of fund clearing functions, communications with relevant parties including participants, dissemination of information, etc.) is sufficient in light of the level and type of the emergency, until the situation

improves. In addition, they shall require the submission of a report based on Article 80(1) of the PSA when necessary.

### **IV-3-3 Operational Risk Management**

#### **(1) Background and Objectives**

Operational Risk is the risk of participants and FCOs incurring losses due to their officers and employees failing to conduct administrative work properly, causing accidents or committing illegal acts in the course of the administrative work process, and is deemed to be caused by various factors, such as information systems and internal procedures, in addition to human errors.

It is important that FCOs pursue sound and appropriate business operations by establishing arrangements and procedures for managing operational risks.

#### **(2) Major Supervisory Viewpoints**

- (i) Whether the FCO has established appropriate policies, procedures, etc. to identify and manage operational risks. Whether the FCO examines them periodically, and reviews them as necessary. Whether the board of directors endorses such policies, procedures, etc., and clearly defines the roles and responsibilities for addressing operational risk. Also, whether the FCO has implemented specific measures to reduce operational risks.
- (ii) Whether the FCO has sufficient processing capacity to achieve a certain level of service in consideration of the volume of administrative processes, etc. expected in the future.
- (iii) In cases where the FCO outsources part of its administrative processes to service providers or other third parties or relies on them, whether the FCO confirms that the outsource fulfills the requirements that would have to be met if such processes were carried out by the FCO itself.
- (iv) Whether the FCO has specified a policy and procedures for selecting the business operations to be outsourced and the contractors to outsource them to, and concluded a contract and developed a control environment that enables sufficient management of such contractors.

#### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the response by the FCO, the supervisory departments shall monitor voluntary business improvement made by the FCO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 80(1) of the PSA.



Furthermore, the supervisory departments shall take actions such as issuing an order for business improvement based on Article 81 of the PSA when the FCO's control environment for managing operational risks is deemed to have a serious problem and the action is deemed to be necessary from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

#### **IV-3-4 Information Technology Risk Management**

##### **(1) Background and Objectives**

Information technology risk is the risk that FCOs, etc. will incur losses generally because of a computer system breakdown, malfunction or other inadequacies, or because of inappropriate or illegal use of computer systems.

FCOs' systems are themselves market infrastructures that are indispensable for fund clearing, etc., so if any system troubles or cybersecurity incidents occur, they may inflict damage on FCOs and participants connected to the systems, and in turn, impact the financial system as a whole.

Therefore, it is important to build a robust control environment for managing information technology risks in FCOs.

(Note) "Cybersecurity incidents" refers to instances of cybersecurity being threatened by so-called cyberattacks, including unauthorized intrusion, theft, modification and destruction of data, failure or malfunction of information systems, execution of illegal computer programs and DDoS attacks, committed via the Internet through malicious use of information communication networks and information systems.

##### **(2) Major Supervisory Viewpoints**

###### **(i) Recognition of Information Technology Risk**

- A. Whether the board of directors or council, etc. has formulated a basic policy for organization-wide management of information technology risk based on a full recognition of information technology risk.
- B. Whether the board of directors or council, etc. recognizes that prevention and efforts for speedy recovery from system troubles and cybersecurity incidents (hereinafter referred to as "system trouble, etc.") is an important issue and has developed an appropriate control environment.
- C. Whether there are arrangements and procedures for ensuring that information regarding information technology risk is properly reported to the management team.

**(ii) Establishment of Appropriate Control Environment for Risk Management**

- A. Whether the FCO has specified a basic policy for the management of information technology risk and developed a relevant control environment.
- B. Whether the FCO has designated the types of risk that should be managed according to specific criteria and has identified the location of the risk.
- C. Whether the control environment for managing information technology risk is effective enough to, enable the FCO to identify and analyze the actual state of its business operations and system troubles, and minimize the frequency and scale of system troubles in a manner suited to the system environment and other factors, thereby maintaining an appropriate level of computer system quality.

**(iii) Assessment of information technology risk**

Whether the division managing information technology risk recognizes and assesses risks periodically or in a timely manner by recognizing the fact that risks are becoming diversified due to changes in the external environment, such as seen in the examples of system troubles induced by large-scale transactions as a result of increased customer channels and efforts to enhance information networks that bring more diverse and broad-based impact.

Also, whether it is taking sufficient measures to address the risks that have been identified.

**(iv) Management of information security**

A. Whether the FCO has developed a policy to appropriately manage information assets, prepared organizational readiness, introduced in-house rules, etc., and developed an internal control environment. Also, whether it is making continuous efforts to improve its information security control environment through the PDCA cycle, taking notice of illegal incidents or lapses at other companies.

B. Whether the FCO is managing information security by designating individuals responsible for it and clarifying their roles/responsibilities in efforts to maintain the confidentiality, integrity and availability of information. Also, whether the individuals responsible for information security are tasked to handle the security of system, data and network management.

C. Whether the FCO is taking measures to prevent unauthorized use of computer systems, unauthorized access, and intrusion by malicious computer programs such as computer viruses.

D. Whether the FCO identifies important information of participants it is responsible

for protecting in a comprehensive manner, keeps its records and manages them.

Whether the FCO, in identifying important information of participants, has set business operations, systems and external contractors as the scope of protection and includes data, such as listed below, in the scope where it tries to identify those calling for protection.

- Data stored in the areas within the system that are not used in ordinary operations
- Data output from the system for analyzing system troubles, etc.

E. Whether the FCO is assessing importance and risks regarding important information of participants that has been identified.

Also, whether it has developed rules to manage information, such as those listed below, in accordance with the importance and risks of each piece.

- Rules to encrypt or mask information
- Rules for utilizing information
- Rules on handling data storage media, etc.

F. Whether the FCO has introduced measures to discourage or prevent unauthorized access, unauthorized retrieval, data leakage, etc. such as listed below, for important information of participants.

- Provision of access authorizations that limits access to the scope necessary for the person's responsibility
- Storage and monitoring of access logs
- Introduction of mutual checking functions such as by separating the individuals in charge of development and those responsible for operations, administrators and those responsible for operations, etc.

G. Whether the FCO has introduced rules for controlling confidential information, such as encryption and masking. Also, whether it has introduced rules regarding the management of encryption programs, encryption keys, and design specifications for encryption programs.

Note that "confidential information" refers to information, such as PIN, passwords, etc., whose misuse could lead to losses by participants.

H. Whether the FCO gives due consideration to the necessity of holding/disposing of, restricting access to, and taking outside, of confidential information, and treats such information in a stricter manner.

I. Whether the FCO periodically monitors its information assets to see whether they are managed properly according to management rules, etc. and reviews the control environment on an ongoing basis.

J. Whether the FCO conducts security education (including by external contractors)

to all officers and employees in order to raise awareness of information security.

**(v) Management of cybersecurity**

- A. Whether the board of directors or council, etc. recognizes the importance of cybersecurity amid increasingly sophisticated and cunning cyberattacks and has introduced the necessary control environment.
- B. Whether the FCO has introduced systems to maintain cybersecurity, such as listed below, in addition to making the organization more secure and introducing in-house rules, etc.
- Monitoring systems against cyberattacks
  - Systems to report cyberattacks and public-relation systems when attacks occur
  - Emergency measures by Computer Security Incident Response Team and systems for early detection
  - Systems of information collection and sharing through information-sharing organizations, etc.
- C. Whether the FCO has introduced a multi-layered defence system against cyberattacks that combines security measures respectively for inbound perimeter control, internal network security control and outbound perimeter control.
- Security measures for inbound perimeter control (e.g. introduction of a firewall, anti-virus software, Intrusion Detection System, Intrusion Protection System etc.)
  - Security measures for internal network security control (e.g. proper management of privileged IDs/passwords, deletion of unnecessary IDs, monitoring of execution of certain commands, etc.)
  - Security measures for outbound perimeter control (e.g. retrieval and analysis of communication/event logs, detecting/blocking inappropriate communication, etc.)
- D. Whether measures such as listed below are implemented to prevent damage from expanding when cyberattacks occur.
- Identification of IP addresses from which the cyberattacks originate and blocking off of attacks
  - Functions to automatically spread out accesses when under DDoS attacks
  - Suspension of the entire system or its part, etc.
- E. Whether necessary measures for vulnerabilities in the system, such as updating of the operating system and application of security patches, are introduced in a timely manner.
- F. Whether the FCO is, as part of cybersecurity measures, assessing its security levels by taking advantage of tests on network intrusion, vulnerability scanning or

penetration tests, etc. and making efforts to improve security.

G. Whether the FCO, when carrying out business operations using communication methods such as the Internet, has introduced appropriate authentication methods in line with the risks associated with such transactions, such as listed below.

-Authentication methods that do not rely on fixed IDs or passwords, such as variable passwords and digital certificates

-Transaction authentication using transaction signatures by means of a hardware token, etc.

H. Whether the FCO, when carrying out business operations using communication methods such as the Internet, has introduced preventative measures in line with operations, such as listed below.

-Introduction of software that allows the FCO to detect the state of virus infection of the participant's system and issue a warning

-Adoption of methods to store digital certificates in mediums or devices separate from systems used in the relevant business operation, such as IC cards

-Introduction of a system that allows the FCO to detect unauthorized log-ins, abnormal input, etc. and immediately notify such abnormalities to participants

I. Whether the FCO has developed contingency plans against potential cyberattacks, conducts exercises and reviews such plans. Also, whether it participates in industry-wide exercises as necessary.

J. Whether the FCO has formulated plans to train and expand the personnel responsible for cybersecurity and implements them.

#### **(vi) System Planning, Development and Operational Management**

A. Whether the FCO has formulated a medium/long-term development plan after having clarified its strategic policy for systems as part of its management strategy. Whether the medium/long-term development plan has been approved by the board of directors or council.

B. Whether the FCO reveals the risks inherent to its existing systems on an ongoing basis, and makes investments to maintain and improve the systems in a planned manner.

C. Whether the FCO has clarified its rules for approval of plans, development and transition in development projects.

D. Whether the FCO specifies the responsible person with respect to each development project and manages the progress based on the development plan.

E. Upon system development, whether the FCO conducts tests in an appropriate and sufficient manner, such as by preparing test plans and making user divisions

participate.

- F. For human resources development, whether the FCO formulates and implements specific plans to pass on the mechanism and development technologies of its existing systems and train personnel with expertise.

**(vii) Computer System Audits**

- A. Whether an internal audit section that is independent from the computer system division conducts periodic audits of the computer system.
- B. Whether the FCO conducts internal audits by subject matter about computer systems and is taking of external audits by information system auditors.
- C. Whether the audited division accounts for all business operations involving information technology risk.

**(viii) Management of Outsourcing of Business Operations**

- A. Whether the FCO selects outsources (including system subsidiaries) by evaluating and examining them based on selection criteria.
- B. Whether the FCO has prescribed the allocation of roles and responsibilities, audit authority, subcontracting procedures, level of services rendered, etc. with the outsource in an outsourcing agreement. Also, whether the FCO presents to outsourced contractors rules and security requirements their officers and employees are required to adhere to and security requirements, as well as defines them in contract forms, etc.
- C. Whether the FCO properly conducts risk management regarding outsourced business operations (including work further subcontracted) related to the computer system. In cases where system-related administrative processes are outsourced, whether the FCO properly conducts risk management according to the outsourced business operations related to the computer system.
- D. Whether the FCO periodically monitors the outsourced business operations (including work further subcontracted) to determine, as the outsourcer, that the outsourced business operations are properly conducted.

Also, whether there is a system that allows the consigner to monitor and track the status of data of participants being processed at outsourced contractors.

**(ix) Contingency Plan**

- A. Whether the FCO has formulated a contingency plan and has established arrangements and procedures for dealing with emergencies.
- B. Whether the FCO is basing the details of its contingency plan on guides that allows it

to judge objective levels of its details (such as "Guide to Formulate Contingency Plans at Financial Institutions" compiled by the Center for Financial Industry Information Systems).

- C. Whether the FCO, in developing a contingency plan, assumes not only contingencies due to natural disasters but also system troubles, etc. due to internal or external factors.

Also, whether it assumes risk scenarios of sufficient extent for cases such as a major delay in batch processing.

- D. Whether the FCO reviews assumed scenarios in its contingency plan by, for example, taking into consideration case studies of system troubles, etc. at other financial institutions, clearing organizations, fund clearing organizations, book-entry transfer institutions and trade repositories, and the results of deliberations at the Central Disaster Management Council, etc.
- E. Whether exercises in accordance with the contingency plan involve the entire company and are periodically conducted jointly with outsourced contractors, etc.
- F. Whether off-site backup systems, etc. are introduced for important systems whose failure could seriously affect business operations, and that a control environment is in place to address disasters, system troubles, etc. so that normal business operations can be speedily brought back.

**(x) Risk of System Updates, etc.**

- A. Whether the FCO has developed a control environment for managing the risk of system updates, etc. by ensuring that its officers and employees fully recognize the risk.
- B. Whether the FCO has established arrangements and procedures for conducting tests. Whether its test plan is suited to the nature of the system development necessitated by the system updates, etc.
- C. Whether the FCO has established a control environment that enables itself to be proactively involved in the system updates, etc. when this task is outsourced.
- D. Whether the FCO makes use of third-party evaluation, such as evaluation by a system auditor, when making judgment regarding important matters related to the system updates, etc.
- E. Whether the FCO has developed a contingency plan for dealing with an unexpected incident.

**(xi) Response to System Troubles**

A. Whether the FCO implements appropriate measures to avoid creating unnecessary confusion among participants, etc. when system troubles, etc. occur and performs tasks towards the prompt recovery and operation of alternatives.

Also, whether it has developed a worst-case scenario in preparation for system troubles and is prepared to take necessary measures accordingly.

B. Whether the FCO has prepared procedures that also subjects outsourced contractors to reporting system troubles, and has a clearly defined system of command and supervision.

C. Whether the FCO is prepared to immediately notify the officers including the representative director and administrative director when a system trouble that may significantly affect business operations occurs, and report the largest potential risk it poses under the worst-case scenario (for example, if there is a possibility that the failure could gravely affect participants, the reporting persons should not underestimate the risk but immediately report the biggest risk scenario).

In addition, whether it is prepared to launch a task force, have the representative director or administrative director, etc. issue appropriate instructions and orders, and seek resolution of the issue in a swift manner.

D. Whether the FCO, after system troubles, etc. have occurred, analyzes the cause and implements measures based on the analysis to prevent recurrence.

Also, whether it periodically analyzes tendencies of factors that have led to system troubles, etc. and introduces measures to address them.

E. Whether the FCO immediately reports system, etc. troubles to the authorities.

### **(3) Supervisory Method and Actions**

#### **(i) At the Time of Problem Recognition**

When supervisory departments have recognized an issue of supervisory concern regarding an FCO's control environment for managing information technology risk, through daily supervisory administration, etc., they shall identify and keep track of the status of voluntary improvement made by the FCO, by holding in-depth hearings with the FCO and the outsourcing contractor and, when necessary, requiring the submission of reports based on Article 80 of the PSA.

When the FCO is deemed to have a serious problem from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner, the supervisory departments shall take actions such as issuing an order for business improvement, etc., based on Article 81 of the PSA.

#### **(ii) At the Time of System Updates, etc.**



In cases where FCOs are to perform system updates, etc., they shall be required to submit specific plans for implementing the system updates, etc. and documents regarding the internal control environment for managing the risk associated with the system updates, etc. (including internal audits) and other matters according to their characteristics.

In cases where the system updates, etc. are large in scale, FCOs shall be required to periodically submit reports based on Article 80(1) of the PSA until such system updates, etc. are completed.

#### **(4) Response to System Troubles**

- (i) FCOs shall be required to notify the authorities of the occurrence of any computer system troubles as soon as they have recognized it, and submit a “Report on Problem Occurrence, etc.” (in the format specified in Attached List of Formats 2-1) to the authorities.

After the computer system operation has been restored to normal and the cause of the problem has been identified, they shall be required to report to the authorities again. (It should be kept in mind that they shall be required to report to the authorities on the current state within one month even if the computer system operation has not been restored to normal or the cause of the problem has not been identified within the one-month period.)

(Note) Computer System Trouble Subject to Reporting to the Authorities

Problems that must be reported to the authorities are those which affect systems and equipment (including both hardware and software) used by FCOs and contractors undertaking business operations outsourced by FCOs, and which could affect the FCOs’ abilities to identify and keep track of the status of transactions, financial settlements, cash deposits and withdrawals, fund-raising and financial conditions, and undermine the convenience of participants, etc. in other ways.

However, the reporting requirement is not applicable to such system troubles in cases where a backup system has started up and effectively prevented adverse effects.

It should be noted that even if no computer system troubles have occurred, a report must be made in cases where participants or business operations will be affected or are highly likely to be affected, including cases where an FCO has received a warning of a cyber-attack on its computer system or where it has detected the possibility of such an attack.

- (ii) An FCO who has reported computer system troubles to the authorities shall be required to submit an additional report based on Article 80(1) of the PSA when necessary. When

the FCO is deemed to have a serious problem from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner, the authorities shall take actions such as issuing an order for business improvement based on Article 81 of PSA

When the FCO is deemed to have committed a serious and malicious violation of law, the authorities shall consider necessary actions, including the issuance of an order for business suspension based on Article 81 of the PSA.

#### **IV-3-5 Procedures to Deal with Participant Default, etc.**

##### **(1) Background and Objectives**

In the event of default, etc. of participants, etc., the FCO needs to promptly take action in order to continue facilitating fund clearing functions, such as disposing of collateral, procuring financial resources to cover the losses and responding in cases where the procurement of additional financial resources becomes necessary.

From this perspective, FCOs are required to clearly establish procedures to deal with default, etc., including their authority and the participants' obligations. FCOs also need to properly verify whether such procedures are actually executable in practice in the event of a participant default, etc.

##### **(2) Major Supervisory Viewpoints**

(i) Whether the FCO has clearly established procedures in its business rules with respect to the funding of financial resources and other matters in the event of a participant default, etc., in order to enable the continuation of smooth business operations such as the performance of obligations of the FCO.

In particular, whether the FCO has clearly defined the amount of financial resources required to cover the losses incurred as a result of a participant default, etc. and the order of its use, as well as the authority to carry out additional collections and the method of allocation in cases where losses that cannot be covered by the funding of prefunded financial resources are incurred.

(ii) Also, whether the FCO tests periodically, at least once a year, and reviews as necessary, the procedures to deal with a participant default, etc. in collaboration with participants and other parties concerned.

(iii) Whether the FCO has developed a manual, etc. to deal with a participant default, etc. and periodically verifies its feasibility with employees involved in the procedures to deal with a participant default, etc., participants and other parties concerned.

(iv) Whether the FCO has established clear rules and procedures to settle payment

obligations in a timely manner even in the event of individual or combined default, etc. among its participants.

**(3) Supervisory Method and Actions**

In cases where a problem has been found in the procedures to deal with a participant default, etc., the supervisory departments shall monitor voluntary business improvement made by the FCO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 80(1) of the PSA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 81 of the PSA when it is deemed necessary to do so from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

**IV-3-6 Management of Collateral, etc.**

**(1) Background and Objectives**

From the viewpoint of ensuring the financial soundness of an FCO, etc., it is important that the collateral provided by participants, etc. is preserved as an asset with sufficiently high creditworthiness and managed properly by the holding entity, and that the collateral is available for use by the FCO promptly at times of emergencies.

**(2) Major Supervisory Viewpoints**

Whether the FCO rigorously selects the entity that will hold the collateral accepted in consideration of said entity's creditworthiness, management arrangements and procedures such as safekeeping procedures, procedures for using collateral at time of emergency, etc.

**(3) Supervisory Method and Actions**

In cases where a problem has been found in the arrangements, procedures, etc. for the Management of Collateral, etc., the supervisory departments shall monitor voluntary business improvement made by the FCO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 80(1) of the PSA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 81 of the PSA if it is deemed necessary to do so from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

#### **IV-3-7 Notes concerning Tiered Structure of Participants, etc.**

##### **(1) Background and Objectives**

There are tiered participation arrangements in which, when using an FCO, a person/entity (indirect participant) uses the FCO's system through another person/entity (direct participant). Such tiered participation arrangements enable more participants to access fund clearing operations as indirect participants through direct participants, while the business structure might become complicated depending on the relationship between direct participants and indirect participants and the nature of the business process, giving rise to various potential risks. FCOs need to identify risks inherent in such tiered participation arrangements and establish appropriate arrangements and procedures for managing such risks.

##### **(2) Major Supervisory Viewpoints**

- (i) Whether the FCO identifies risks involved in tiered participation arrangements and takes measures to manage such risks in its rules, procedures, etc., such as gathering basic information about indirect participation.
- (ii) Whether the FCO examines the risks with respect to direct participants with indirect participants' positions that account for a high ratio relative to their financial position identified by gathering information as referred to above or by other means, direct participants, etc. serving as a settlement intermediary for a large number of financial institutions.
- (iii) Whether the FCO regularly examines risks to the FCO that may arise in the event of the default of an indirect participant, and takes action to mitigate such risks when necessary and appropriate.

##### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the arrangements and procedures for managing risks arising from tiered participation arrangements, etc., the supervisory departments shall monitor voluntary business improvement made by the FCO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 80(1) of the PSA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 81 of the PSA when it is deemed necessary to do so from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

## **IV-3-8 Appropriateness of Disclosure of Information, etc.**

### **(1) Background and Objectives**

It is important that FCOs provide sufficient information so that participants and prospective participants can clearly recognize and fully understand the risks and responsibilities arising from their participation in the fund clearing system.

Furthermore, from the viewpoint of providing sufficient information to participants, etc., it is important that the rights and obligations of participants, etc. and key procedures concerning risks, etc. are clarified and publicly disclosed in business rules and other rules and procedures.

### **(2) Major Supervisory Viewpoints**

- (i) Whether the FCO has formulated clear and comprehensive rules and procedures and disclosed them to participants. Whether the FCO publicly discloses key rules, procedures, etc.
- (ii) In the aforementioned rules, procedures, etc., whether the FCO clearly describes the rights and obligations of the FCO and participants, so that participants can assess the risks they would incur by participating in the FCO.
- (iii) Whether the FCO clarifies operations performed at a charge and operations performed without charge, and publicly discloses the fee and content of individual services.
- (iv) Whether the FCO periodically discloses information based on the “Principles for Financial Market Infrastructures” and the “Disclosure framework and Assessment methodology”<sup>(Note)</sup> that supplements the principles.

(Note) CPSS and IOSCO, “Disclosure framework and Assessment methodology” (December 2012)

### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the disclosure of major rules, etc. by the FCO, the supervisory departments shall monitor voluntary business improvement made by the FCO, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 80(1) of the PSA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 81 of the PSA when it is deemed necessary to do so from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.

## **IV-4 Various Administrative Procedures**

### **IV-4-1 Points to Consider regarding Authorization of Business Rules, etc.**

#### **(1) Background and Objectives**

Business rules prescribe the desirable status of business operations of an FCO, as well as basic matters regarding the FCO's clearing system, such as measures that can be taken by the FCO with respect to participants, including requirements for participants, assuming authorization by the authorities.

In light of the above, FCOs are required to clearly establish rules and procedures, etc. for business rules and clarify their basis and characteristics so that clearing of claims and liabilities related to exchange transactions can be performed by participants in a smooth, continuous, and stable manner.

#### **(2) Major Supervisory Viewpoints**

- (i) When making amendments, etc. to business rules, whether the FCO confirms that the fund clearing system as a whole, including business rules and subordinate rules, is consistent with laws and regulations, etc.
- (ii) Whether the FCO discloses and explains such amendment, etc. to participants, participants' customers, etc. in a clear and easy-to-understand manner at least after receiving authorization by the authorities, or as necessary, before then.
- (iii) When giving such explanation, whether the FCO explains the effectiveness and the priority of contracts in the event of a participant default, etc. by summarizing the basis and applicability of laws and regulations pertaining to contracts on fund clearing, etc.
- (iv) In cases where there is a foreign participant or in cases where assets are held abroad, such as collateral for fund clearing, whether the FCO confirms the risks associated with differences in laws and regulations, such as whether or not the effectiveness of contracts would be undermined in the event of default, etc., including by confirming the laws and regulations, etc. of the country concerned.
- (v) When confirming and explaining the above, whether the FCO gives consideration to the accuracy of such confirmation and explanation by such means as utilizing outside experts as necessary.
- (vi) In the rules for business rules, etc., whether the FCO has clarified the point at which settlement is final in its rules and procedures. Also, whether the FCO has clarified at what point unsettled payment, transfer instruction or other obligation becomes irrevocable by participants.

(vii) Whether the FCO confirms that the provisions on the above are consistent with laws and regulations, etc. and explains them to participants, participants' customers, etc.

#### **IV-4-2 Points to Consider regarding Approval of Subsidiary Business**

##### **(1) Purpose**

If the soundness of an FCO is not ensured, there is a risk that not only the stability of the FCO's operations, but also the soundness of the financial system as a whole may be undermined through management concerns, etc. of the FCOs (i.e., systemic risk).

Considering their highly public nature as such, FCOs must concentrate on fund clearing operations and business related thereto,<sup>(Note)</sup> and in principle, are not able to conduct any other business, for the purpose of blocking out risks from operations other than their core business (Article 69(1) of the PSA).

On the other hand, based on the view that the provision of services other than their primary business may help improve the convenience, stability, etc. of the settlement system as a whole, even if they do not correspond to fund clearing operations or business related thereto, FCOs are able to conduct business that is found to have no risk of hindering their conducting of fund clearing operations appropriately and certainly, as related business, by obtaining approval.

(Note) What consists of business related to fund clearing operations needs to be examined with respect to each individual business, considering that the fund clearing operations are aimed at clearing claims and liabilities related to exchange transactions conducted between banks. For example, the sending and receiving of payment instruction information related to exchange transactions and settlement information related to the clearing balance, the maintenance, management, etc. of information systems necessary for processing such information, and peripheral administrative processes related to fund clearing operations are deemed to correspond to businesses related to fund clearing operations.

##### **(2) Application for Approval**

Upon making an application for approval, the FCO shall submit the approval application form prescribed in Article 5(1) of the Cabinet Office Ordinance on Financial Instruments FCOs, etc. (Attached List of Formats) and the attached documents listed in the items of Article 15(2) of said Ordinance.

##### **(3) Approval Screening**

Upon approval screening, it is necessary to determine the appropriateness of approval on a case-by-case basis, in view of such matters as whether there is a risk of hindering the FCO from conducting fund clearing operations appropriately and certainly. Specifically, approval screening shall be conducted from the following viewpoints.

- (i) Whether there is a high likelihood of causing losses for the FCO and affecting its management.
- (ii) Whether the FCO has identified the risks to which it will be exposed and has established arrangements and procedures for managing such risks properly.
- (iii) Whether there is a risk of undermining confidence in the fairness and impartiality of the clearing operations or undermining the social credibility as an FCO.
- (iv) Whether the workload hinders the appropriate operation of the fund clearing operations.

#### **(4) Supervisory Method and Actions after Granting Approval**

FCOs are important social infrastructures that ensure speedy and reliable means of settlement, and authorities are required to conduct monitoring on an ongoing basis so that the sound and appropriate operation of their primary business is not hindered due to other business operations, say, as a result of confidence in FCOs being undermined.

In cases where other business conducted by an FCO is hindering or has the risk of hindering the sound and appropriate operation of its primary business, the supervisory departments shall monitor voluntary business improvement made by the FCO, by holding an in-depth hearing and, when necessary, requiring the submission of a report based on Article 80(1) of the PSA.

Furthermore, the supervisory departments shall consider taking actions, such as issuing an order for business improvement under the provision of Article 81 of the PSA when it is deemed necessary to do so from the viewpoint of conducting fund clearing operations in an appropriate and reliable manner.



## **V. Supervisory Viewpoints and Procedures (Book-entry Transfer Institutions)**

### **V-1 Governance / Business Administration**

#### **V-1-1 Governance System**

##### **(1) Background and Objectives**

As BeTIs perform a huge quantity and value of post-trade processes for financial transactions of securities, including custody and book-entry transfer of securities, they play an important role in facilitating the circulation of securities. Under these circumstances, there shall be effective disciplines for management and proper governance in BeTIs, in order to ensure appropriate and secure implementation of BeTIs' business operations, and in turn, financial system stability.

Effective functioning of governance presumes that the components of the organization are fulfilling their primary roles. Specifically, it is important that, for example, organs such as the board of directors and the board of auditors are able to check management, and checks and balances among divisions are functioning properly, as is the internal audit section. It is also necessary for representative directors, directors, executive officers, auditors and employees in all positions to understand their respective roles and be fully involved in the process.

(Note) In the case of BeTIs that have established nominating committees, etc., it is necessary to examine whether the board of directors, nominating committees, executive officers, etc. are properly exercising their respective authority appropriately. In addition, in the case of BeTIs that have established an audit and supervisory committee, it is necessary to examine whether the board of directors and audit and supervisory committee, etc. are properly exercising their respective authority. In this case, examination should be conducted with due consideration of the actual status of management based on the purpose of these Guidelines.

##### **(2) Major Supervisory Viewpoints**

###### **[Representative Director]**

- (i) Whether the representative director considers compliance as one of the important management issues and takes the initiative in building a control environment for compliance.
- (ii) Whether the representative director fully recognizes that disregarding the risk

management division may have a serious impact on corporate earnings and attaches importance to the said division.

**[Directors/Board of Directors]**

- (i) Whether directors check and prevent autocratic management by the representative director and other officers who are responsible for business execution, and are actively involved in the board of directors' decision-making and checking process concerning business execution.
- (ii) In cases where outside directors are appointed, whether they recognize their own significance from the viewpoint of ensuring objectivity in the decision-making of management, etc. and proactively participate in the meetings of the board of directors. In cases where proposals for the appointment of outside directors are to be determined, whether the outside directors' personal relationships and equity relationships with the BeTI and other interests are verified and their independence, aptitude, etc. are carefully examined, in consideration of the roles they are expected to fulfill. Whether some kind of framework has been established so that outside directors would make appropriate judgments at the meetings of the board of directors; for example, whether information is provided on an ongoing basis.
- (iii) Whether the board of directors takes measures to objectively ensure the appropriateness and fairness of, for example, important management decisions and management judgments related to compliance, etc., such as utilizing the advice of outside experts and discretionary committees whose members consist of outside experts as necessary when making such decisions and judgments. In particular, whether the board of directors takes measures to appropriately reflect the **legitimate interests** of its participants and other relevant stakeholders on design, rules, overall strategy, and major decisions.
- (iv) Whether the board of directors has specified a management policy based on the overall vision of the desirable status of the BeTI. Whether it has established management plans in line with the management policy and communicated the plans throughout the organization. Whether it regularly reviews and revises the progress status thereof.
- (v) Whether directors and the board of directors are sincerely leading efforts in compliance and are properly demonstrating the board's functions to establish an organization-wide internal control environment.
- (vi) Whether the board of directors fully recognizes that disregarding the risk management division may have a serious impact on corporate earnings, and attaches importance to the said division. In particular, whether the director in charge has in-depth knowledge and

understanding concerning the methods of measuring, monitoring and managing risks, in addition to an understanding of where risks reside and what kind of risks they are.

- (vii) Whether the board of directors has set up a policy for managing risks based on strategic objectives and communicated it throughout the organization. Whether it reviews the risk management policy on a periodic or as-needed basis. In addition, whether the board of directors makes use of risk-related information in the execution of business and the development of risk management systems by, for example, making necessary decisions based on the status of risks reported periodically.

**[Auditors/Board of Auditors]**

- (i) Whether the independence of the auditors and the board of auditors is ensured in accordance with the purpose of the board of auditors system.
- (ii) Whether the auditors and the board of auditors properly exercise the broad authority granted thereto and conduct audits of business operations in addition to audits of accounting affairs.
- (iii) Whether individual auditors recognize the importance of their own independence within the board of auditors and actively take the initiative to conduct audits.
- (iv) Whether the auditors and the board of auditors strive to ensure the effectiveness of their audits by, for example, receiving reports on the results of external audits, depending on the contents thereof.

**[Internal Audit Section]**

- (i) Whether the internal audit section is independent from divisions subject to audit so as to fully check the actions thereof, has the control environment and ability to collect important information on their operational status, etc. in a timely manner, and is sufficiently staffed and equipped to conduct effective internal audits that are accurately adapted to the environment surrounding the BeTI and its operational status.
- (ii) Whether the internal audit section formulates efficient and effective internal audit plans that give consideration to frequency and depth according to the type and magnitude of risks based on its understanding of the status of risk management, etc. by divisions subject to audits, properly reviews the plans depending on the situation, and conducts efficient and effective internal audits based on the internal audit plans.
- (iii) Whether the internal audit section reports important issues pointed out in internal audits without any delay to the representative director and the board of directors. Whether the internal audit section has accurately identified the status of improvements made on the issues pointed out.

**[Use of External Audits]**

- (i) Whether external audits are effectively utilized, with sufficient understanding that effective external audits are indispensable for ensuring sound and appropriate business operations of BeTIs.
- (ii) Whether external audits are examined periodically as to whether they are effectively functioning, and appropriate measures are taken with respect to the external audit results, etc.
- (iii) Whether such matters as the number of consecutive years of service by a certified public accountant involved are handled properly.

**(3) Supervisory Method and Actions**

Supervisory departments shall examine the status of governance through the following hearings and daily supervisory administrative processes.

**(i) Comprehensive Hearings (See II-1-1 (1))**

Supervisory departments shall hold hearings regarding BeTIs' management challenges, strategies and the status of risk management and governance, among other matters. In addition, senior supervisory departments shall directly hold hearings with top managers of BeTIs as necessary.

**(ii) Examination of Governance through Daily Supervisory Administrative Processes**

Supervisory departments shall examine the effectiveness of governance not only through the hearings described above but also through daily supervisory administrative processes, such as follow-up on reports on business improvements made on matters pointed out in inspections.

**(iii) Recording of Monitoring Results**

Supervisory departments shall compile and store records on matters of particular note based on the results of monitoring conducted through procedures described above, and make effective use thereof in future supervisory administrative processes.

**(iv) Supervisory Method and Actions**

In cases where doubt has arisen about the effectiveness of a BeTI's governance, the supervisory departments shall monitor voluntary business improvement made by the BeTI, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 20 (1) of the Book-Entry Transfer Act.

Furthermore, the supervisory departments shall take actions, such as issuing an order for business improvement based on Article 21 of the Book-Entry Transfer Act, when it is

deemed necessary to do so from the viewpoint of conducting book-entry transfer operations in an appropriate and reliable manner.

## **V-1-2 Officers of Book-entry Transfer Institutions**

### **(1) Major Supervisory Viewpoints**

From the viewpoint of maintaining the public nature of book-entry transfer operations, supervisory departments shall pay attention to the following points when examining the decision-making process regarding proposals for the appointment of officers of the BeTI, among others.

- (i) The officer shall neither meet any of the ineligibility criteria (Article 3(1)(iv)(a) to (f) of the Book-Entry Transfer Act) nor have met any of them at the time when the BeTI was specified as an entity engaged in book-entry transfer operations.
- (ii) The officer shall neither have violated laws and regulations regarding book-entry transfer operations or business incidental thereto nor have breached any administrative actions taken based on laws and regulations.
- (iii) The officer shall not have engaged in an illegal or markedly inappropriate act regarding book-entry transfer operations under particularly grave circumstances.

### **(2) Supervisory Method and Actions**

Supervisory departments shall consider taking actions, such as ordering the dismissal of an officer of a BeTI under the provision of Article 22(1) of the Book-Entry Transfer Act when said officer: (i) meets any criteria specified in Article 3(1)(iv)(a) to (f) of the Book-Entry Transfer Act, or is found to have already met such criteria at the time when the BeTI was specified as an entity engaged in book-entry transfer operations; (ii) is found to have become an officer of the BeTI by fraudulent means; or (iii) violates or is found to have violated laws and regulations or administrative actions taken based on laws and regulations.

In addition, they shall hold an in-depth hearing regarding the decision-making process concerning the proposal for the appointment of the said officer or committee member and, when necessary, require the submission of a report based on Article 20(1) of the Book-Entry Transfer Act. Furthermore, supervisory departments shall consider taking actions, such as issuing an order for business improvement (Article 21 of the Book-Entry Transfer Act), if the BeTI's control environment for governance is deemed to have a serious problem and the action is deemed to be necessary from the viewpoint of conducting book-entry transfer operations in an appropriate and reliable manner.

## **V-1-3 Staffing**

### **(1) Major Supervisory Viewpoints**

Supervisory departments shall examine whether BeTIs are adequately staffed to properly and reliably conduct book-entry transfer operations, in light of the following requirements regarding BeTIs' officers and employees.

- (i) Whether the BeTIs has secured officers and employees who understand the viewpoints regarding governance that are specified under the Book-Entry Transfer Act and other relevant regulations, as well as these Guidelines, and who have the knowledge and experience necessary for conducting governance as well as sufficient knowledge and experience concerning the control environment for compliance, etc. required to properly and reliably conduct book-entry transfer operations.
- (ii) Whether officers or employees are current or former members of organized crime groups or have a close relationship with organized crime groups.
- (iii) Whether officers or employees have the experience of being sentenced to a fine (including similar punishments imposed under foreign laws and regulations equivalent thereto) for violation of the Book-Entry Transfer Act or other domestic financial laws and regulations or foreign laws and regulations equivalent thereto.
- (iv) Whether officers or employees have the experience of being sentenced to a fine (including similar punishments imposed under foreign laws and regulations equivalent thereto) for violation of the Act on Prevention of Unjust Acts by Organized Crime Group Members (excluding the provisions of Article 32-3(7) and Article 32-11(1) of said Act) or other foreign laws and regulations equivalent thereto, or for committing a crime prescribed under the Penal Code or under the Act on Punishment of Physical Violence and Others.
- (v) Whether officers or employees have the experience of being sentenced to imprisonment with work or more severe punishment (including similar punishments imposed under equivalent foreign laws or regulations). In particular, whether officers or employees have been accused of committing crimes specified under Articles 246 to 250 of the Penal Code (fraud, fraud using computers, breach of trust, quasi fraud and extortion, as well as attempts at these crimes).

### **(2) Supervisory Method and Actions**

The requirements specified in (i) to (v) above are part of a comprehensive set of elements that should be taken into consideration when supervisory departments examine

whether a BeTI is adequately staffed to properly and reliably conduct book-entry transfer operations. Even if an officer or an employee is deemed to not meet the requirements, it should not automatically lead to the conclusion that the BeTI is not adequately staffed. The important thing is, first and foremost, that BeTIs strive to ensure on their own responsibility that they are adequately staffed, in light of those requirements and other elements.

However, supervisory departments shall hold in-depth hearings regarding the BeTI's awareness of such staffing and the decision-making process concerning the proposed appointments of officers and employees, in cases where a BeTI is deemed to have failed to take those elements into consideration sufficiently in the said decision-making process, and where it is deemed to be necessary to hold such hearings in relation to the business operations of the BeTI from the viewpoint of properly and reliably conducting book-entry transfer operations protecting the public interest and investors. In addition, they shall require the submission of reports under the provision of Article 20(1) of the Book-Entry Transfer Act when necessary.

Supervisory departments shall consider taking actions, such as issuing an order for business improvement under Article 21 of the Book-Entry Transfer Act, in cases where the BeTI's control environment for governance is deemed to have a serious problem as a result of the examination of the submitted report, and where the action is deemed to be necessary from the viewpoint of properly and reliably conducting book-entry transfer operations.

## **V-2 Financial Soundness**

### **V-2-1 Adequacy of Capital**

#### **(1) Background and Objectives**

In order for BeTIs to gain participants' and market players' confidence and to operate their business continuously and stably, it is important for BeTIs to retain a sufficient financial basis according to the characteristics of management as well as to establish appropriate arrangements and procedures for managing operational risks and other risks.

Accordingly, BeTIs should hold enough liquid assets to withstand any losses that may be incurred in the event that various risks are actualized.

BeTIs also need to have a process for evaluating their capital adequacy in the context of their risk profiles, and implement appropriate measures for maintaining a sufficient level of capital.

#### **(2) Major Supervisory Viewpoints**

##### **[Directors/Board of Directors]**

- (i) Whether the directors have a general understanding of the nature and level of the risks taken by the BeTI as well as the relationship between risk and the appropriate level of capital.
- (ii) Whether the directors and the board of directors understand that, in order to achieve their strategic objectives, a capital plan, which is consistent with them, is an essential component, and whether they have formulated an appropriate capital plan according to the management issues of the BeTI.
- (iii) Whether the directors have been sufficiently involved in formulating the aforementioned capital plan, and are adopting a process for evaluating capital adequacy and implementing appropriate measures for maintaining a sufficient level of capital.

##### **[Capital Adequacy]**

- (i) Upon formulating the aforementioned capital plan, whether the BeTI evaluates the adequacy of capital relative to the risks measured in consideration of changes in the business environment, etc.
- (ii) As for the amount of assets (e.g. the amount of net assets) to be held to prepare against business risks, whether the BeTI has secured at least six months worth of operating expenditures and examined the sufficiency of the level of such amount in consideration of ensuring the BeTI's business continuity.



- (iii) Whether the BeTI properly examines equity capital, for example, as to whether the equity capital consists primarily of cash and cash equivalents, etc. and can thus be easily liquidated in a stress scenario.
- (iv) Whether the BeTI has a feasible plan to raise additional capital if the level of capital approaches or falls below levels that would make its business continuity uncertain.

## **V-2-2 Risk Management Framework**

### **(1) Background and Objectives**

BeTIs function as the core of the securities settlement system through recording and management of transfer account books with special legal effects. Therefore, when conducting business operations, they are required to recognize that they face not only operational risks such as administrative errors and information leakage but also various other risks, including information technology risk, comprehensively check whether or not such risks affect its business operations, and establish appropriate arrangements and procedures for managing risks.

### **(2) Major Supervisory Viewpoints**

- (i) Whether the risk management division has sufficient authority, independence, resources, and access to the board in order to conduct effective risk management. For example, whether the reporting lines for risk management are clear and separate from those for other operations of the BeTI, so that the matters can be directly reported to the board of directors by the authority of the risk management division.
- (ii) Whether the BeTI has revealed and identified all risks in order to grasp diverse risks in a comprehensive manner, and if possible, has properly determined risk categories to place them under quantitative risk management.
- (iii) Whether the BeTI reviews the scope of quantification and accuracy to improve them as necessary. For example, whether the BeTI reviews the importance, correlation, etc. of different types of risks to ensure appropriateness.
- (iv) Whether the board of directors has clearly set up a policy for managing risks based on strategic objectives in accordance with the management policy of the BeTI as a whole, and examines the policy periodically, at least annually, and revises it as necessary. In addition, whether the board of directors takes appropriate measures to make the risk management policy widely known within the organization.
- (v) Whether the board of directors makes use of risk-related information in the execution of business and the development of risk management systems by, for example, making

necessary decisions based on risk status reports received periodically.

- (vi) In Japan, the book-entry transfer system is operated under the Book-Entry Transfer Act; as for the treatment of foreign shores etc., the BeTI manages custody risk through appropriate rules and procedures as necessary.
- (vii) Whether the BeTI takes measures to identify and manage potential sources of risk arising from the set of contractual and operational arrangements among other financial market infrastructures that connect the BeTI directly or through an intermediary before entering into such arrangements, and on an ongoing basis once such arrangements are established.

### **V-2-3 Supervisory Method and Actions**

In cases where a problem has been recognized with regard to the financial soundness of a BeTI, the supervisory departments shall monitor voluntary business improvement made by the BeTI, by holding an in-depth hearing regarding the cause of the problem and improvement measures and, when necessary, requiring the submission of a report based on Article 20(1) of the Book-Entry Transfer Act.

Furthermore, the supervisory departments shall take actions, such as issuing an order for business improvement based on Article 21 of the Book-Entry Transfer Act when it is deemed necessary to do so from the viewpoint of properly and reliably conducting book-entry transfer operations.

## **V-3 Operational Appropriateness**

### **V-3-1 Compliance**

#### **V-3-1-1 Measures for Ensuring Compliance**

##### **(1) Notes Regarding Policies, Procedures, etc. Pertaining to Compliance**

- (i) Whether the BeTI regards compliance as one of the most important issues for management, and whether it has formulated a basic policy concerning the implementation of compliance, as well as a detailed implementation plan (compliance program) and a code of conduct (ethics code, compliance manual), etc.
- (ii) Whether the BeTI has clearly established the authority and responsibility of the chief compliance officer, and whether there is a system in place for his/her function to be fully exercised.
- (iii) Whether the BeTI has established a system for communicating and reporting compliance-related information appropriately among the management team, the divisions in charge of the book-entry transfer operations, and the compliance division, chief compliance officer or other person in charge.

##### **(2) Notes Regarding the Whistle-blowing System**

- (i) Whether the BeTI has clearly designated the division in charge of the whistle-blowing system and established specific procedures for handling internal allegations, so as to ensure that they are processed and a response is made in a prompt and appropriate manner.
- (ii) Whether the BeTI has developed a system wherein information on the content of internal allegations can be shared within a necessary and appropriate scope.
- (iii) Whether the BeTI makes sure to properly follow up on how internal allegations are being handled.
- (iv) Whether the BeTI accurately and appropriately records and stores the details of internal allegations and the results of investigations thereof, and whether it makes full use of this information such as to improve its operational control system and to formulate measures for preventing a recurrence.

#### **V-3-1-2 Fair Participation Requirements, etc.**

##### **(1) Background and Objectives**

Given the role of BeTIs, which is to contribute to the stable and efficient business operations of Transfer Account Management Institutions (AMIs), etc. by performing a huge quantity and amount of post-trade processes for financial transactions of securities, BeTIs' services should be fair and open to AMIs and other BeTIs, etc.

At the same time, BeTIs are required to establish reasonable participation requirements and manage risks of AMIs to which BeTIs are exposed, in order to ensure their own financial soundness and conduct book-entry transfer operations in a stable manner.

## **(2) Major Supervisory Viewpoints**

- (i) Whether the BeTI has established reasonable participation requirements for AMIs.
- (ii) Whether the BeTI examines whether such participation requirements are fair or not from the viewpoint of properly and reliably conducting book-entry transfer operations, etc., and releases the participation requirements to the public in consideration of such examination.
- (iii) Whether the BeTI abuses its position in such circumstances as using information received from book-entry transfer operations in other services and concluding contracts on services incidental to book-entry transfer operations.
- (iv) Whether the BeTI periodically monitors whether or not AMIs hinder the assurance of appropriate and smooth management of book-entry transfer operations in light of the participation requirements. Whether the BeTI has clearly defined and publicly disclosed procedures for facilitating the suspension and exit of participants in book-entry transfer when necessary and appropriate to do so.

## **(3) Supervisory Method and Actions**

In cases where a problem has been found in the participation requirements or compliance monitoring, the supervisory departments shall monitor voluntary business improvement made by the BeTI, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 20(1) of the Book-Entry Transfer Act.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 21 of the Book-Entry Transfer Act when it is deemed necessary to do so from the viewpoint of properly and reliably conducting book-entry transfer operations.

### **V-3-1-3 Prevention of Damage that May be Inflicted by Anti-Social Forces**

## **(1) Background and Objectives**

Eliminating anti-social forces from society is a task critical to ensuring the order and safety of society, so it is necessary and important to promote efforts to ban any relations with anti-social forces from the viewpoint of fulfilling social responsibility. In particular, as BeTIs are highly public in nature and play an important economic role, they need to exclude anti-social forces from financial instruments markets in order to prevent damage from being inflicted not only on themselves and their officers and employees but also on various stakeholders who participate in financial instruments markets.

Needless to say, if BeTIs are to retain public confidence and maintain the soundness and appropriateness of their business operations, it is essential that they deal with anti-social forces in accordance with laws and regulations without bowing to pressure from them. Therefore, BeTIs must strive, on a daily basis, to develop a control environment for banning any relations with anti-social forces in accordance with the purpose of the “Guideline for How Companies Prevent Damage from Anti-Social Forces” (agreed upon at a meeting on June 19, 2007, of cabinet ministers responsible for anti-crime measures).

In particular, anti-social forces have become increasingly sophisticated in their efforts to obtain funds, disguising their dealings as legitimate economic transactions through the use of affiliated companies in order to develop business relations with ordinary companies. In some cases, the relations thus developed eventually lead to problems. In order to deal with such cases properly, the management teams of BeTIs need to take a resolute stance and implement specific countermeasures.

It should be noted that if a BeTI delays specific actions to resolve a problem involving anti-social forces on the grounds that unexpected situations, such as the safety of officers and employees being threatened, could otherwise arise, the delay could increase the extent of the damage that may be ultimately inflicted on the BeTI.

(Reference) “Guideline for How Companies Prevent Damage from Anti-Social Forces”  
(agreed upon at a meeting on June 19, 2007, of cabinet ministers responsible  
for anti-crime measures)

### **(i) Basic Principles on Prevention of Damage that may be Inflicted by Anti-social Forces**

- Institutional response
- Cooperation with external expert organizations
- Ban on any relations, including transactions, with anti-social forces
- Legal responses, both civil and criminal, in the event of an emergency
- Prohibition of engagement in secret transactions with and provision of funds to anti-social forces

## **(ii) Identification of Anti-social Forces**

In judging whether specific groups or individuals constitute “anti-social forces,” which are defined as groups or individuals that pursue economic profits through the use of violence, threats and fraud, it is necessary not only to pay attention to whether they fit the definition in terms of their affiliation, such as whether they constitute or belong to *boryokudan* crime syndicates, *boryokudan* affiliated companies, *sokaiya* racketeer groups, groups engaging in criminal activities under the pretext of conducting social campaigns or political activities and crime groups specialized in intellectual crimes, but also to whether they fit the definition in terms of the nature of their conduct, such as whether they are making unreasonable demands that go beyond the limits of legal liability. (Refer to the “Key Points of Measures against Organized Crime,” a directive issued in the name of the Deputy Commissioner-General of the National Police Agency on December 22, 2011.)

## **(2) Major Supervisory Viewpoints**

A BeTI should not have any relations with anti-social forces and, in cases where it has established a relationship with an anti-social force unwittingly, supervisors, while also giving consideration to the characteristics of specific transactions, shall pay attention to such as the following points in order to examine its control environment for banning any relations with anti-social forces as soon as possible after the counterparty has been found to be an anti-social force and its control environment for dealing with unreasonable demands by anti-social forces appropriately.

### **(i) Institutional response**

In light of the need and importance of an action to ban any relationship with anti-social forces organically, whether the responsibility of responding to the situation is not left solely to the relevant individuals or divisions but the management including directors are appropriately involved, and there is a policy for the entire organization to respond. In addition, whether there is a policy calling for the corporate group as a whole, not just the involved BeTI alone, to take on an effort to prevent any relationship with anti-social forces.

Furthermore, whether the BeTI is also making efforts to eliminate anti-social forces when conducting transactions including the provision of financial services under business alliance with other companies outside of the corporate group.

### **(ii) Developing of a Centralized Control Environment through anti-social forces response division**

Whether the BeTI has established an anti-social forces response division so as to develop a centralized control environment for preventing anti-social forces from

inflicting damage, and whether this division is properly functioning.

In particular, whether the BeTI pays sufficient attention to the following points in developing the centralized control environment.

- A. Whether the anti-social forces response division is actively collecting and analyzing information on anti-social forces and has developed a database to manage such information in a centralized manner and further, has a system to appropriately update it (i.e., addition, deletion or change of information in the database). Further, whether the division is making efforts to share information within the group in the process of collecting and analyzing such information. Whether the anti-social forces response division has a system to appropriately take advantage of such information for screening the counterparties of transactions and evaluating the attributes of shareholders of the BeTI.
- B. Whether the BeTI makes sure to maintain the effectiveness of measures to ban any relations with anti-social forces by, for example, having the anti-social forces response division develop a manual for dealing with anti-social forces, provide on-going training, foster cooperative relationships with external expert organizations such as the police, the National Center for the Elimination of Boryokudan, and lawyers on an ongoing basis. In particular, whether the BeTI is prepared to report to the police immediately when it faces the imminent prospect of being threatened or becoming the target of an act of violence, by maintaining close communications with the police on a daily basis so as to develop a systematic reporting system and build a relationship that facilitates cooperation in the event of a problem.
- C. Whether the BeTI has a structure in which relevant information is appropriately conveyed to the anti-social forces response division for consultation when transactions with anti-social forces are found or such forces have made unreasonable demands. Further, whether the anti-social forces response division has a structure to appropriately report relevant information to the management. In addition, whether the anti-social forces response division has a structure to ensure the safety of individuals encountering anti-social forces in person and to support divisions involved in dealing with them.

**(iii) Execution of Appropriate Prior Screening**

Whether the BeTI bans allowing anti-social forces to become a participant or counterparty to a transaction by conducting appropriate advance screening using information on such forces in order to prevent transactions with anti-social forces, and makes sure provisions regarding the exclusion of “boryokudan” crime syndicates are introduced in all contracts and terms of transactions.

**(iv) Execution of Appropriate Follow-up Review**

Whether, for the purpose of making sure any relationships with anti-social forces are eliminated, there is a structure to conduct an appropriate follow-up review on existing claims and contracts.

**(v) Measures to Terminate Transactions with Anti-Social Forces**

A. Whether the BeTI has a system under which information confirming the existence of a transaction with anti-social forces is appropriately reported to the management, including directors, etc., via the anti-social forces response division, and responds to the situation under appropriate directions and involvement by the management.

B. Whether the BeTI regularly communicates with external expert organizations, including the police, the National Center for the Elimination of Boryokudan, lawyers and so forth, and promotes efforts to eliminate any transactions with anti-social forces.

C. Whether the BeTI, when it has learned through a follow-up review after initiating a transaction that the counterparty is a member of an anti-social force, takes measures to prevent the provision of benefits to anti-social forces, such as seeking collection to the extent possible.

D. Whether the BeTI has a structure to prevent providing funds or engaging in inappropriate or unusual transactions for whatever reason if the counterparty has been found to be an anti-social force.

**(vi) Dealing with Unreasonable Demands by Anti-Social Forces**

A. Whether the BeTI has a system under which the information that anti-social forces have made unreasonable demands is immediately reported to the management including directors, etc. via the anti-social forces response division and responds to the situation under appropriate directions and involvement by the management.

B. Whether the BeTI actively consults external expert organizations such as the police, the National Center for the Elimination of Boryokudan, and lawyers, when anti-social forces make unreasonable demands, and responds to such unreasonable demands based on guidelines set by the Center for Removal of Criminal Organizations and other organizations. In particular, whether the BeTI has a structure to report to the police immediately when there is an imminent prospect of a threat being made or an act of violence being committed.

C. Whether the BeTI, in response to unreasonable demands by anti-social forces, has a policy to take every possible civil legal action and to avoid hesitating to seek the initiation of a criminal legal action by proactively reporting damage to the authorities.

D. Whether the BeTI ensures that the division in charge of handling problematic conduct promptly conducts a fact-finding investigation upon request from the anti-social forces



response division, in cases where the unreasonable demand from anti-social forces is based on problematic conduct related to business activity or involving an officer or employee.

**(vii) Management of Shareholder Information**

Whether the BeTI manages shareholder information properly, through means such as checking the transaction status of its own shares and examining information regarding the attributes of its shareholders.

**(3) Supervisory Method and Actions**

When supervisory departments have recognized an issue of supervisory concern regarding a BeTI's control environment for banning any relations with anti-social forces, through inspection and daily supervisory administration, they shall identify and keep track of the status of voluntary improvement made by the BeTI by holding in-depth hearings and, when necessary, requiring the submission of reports based on Article 20(1) of the Book-Entry Transfer Act. When the BeTI is deemed to have a serious problem from the viewpoint of properly and reliably conducting book-entry transfer operations, because its internal control environment is extremely fragile, as shown by, for example, a failure to take appropriate steps toward dissolving relations with anti-social forces despite recognizing the provision of funds thereto and the presence of inappropriate relations therewith, supervisory departments shall take actions such as issuing an order for business improvement based on Article 21 of the Book-Entry Transfer Act.

**V-3-1-4 Verification at the Time of Transaction and Reporting of Suspicious Transactions**

**(1) Background and Objectives**

From the viewpoint of preventing abuse of financial services by organized crime groups and maintaining public confidence in Japan's financial markets, it is important to establish an internal control environment for measures such as verification at the time of transaction (meaning such measures as verification at the time of transaction provided in Article 11 of the Act on Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007; hereinafter referred to as the "Anti-Criminal Proceeds Act"); the same applies hereinafter) based on that Act .

**(2) Major Supervisory Viewpoints**

- (i) Whether the BeTI has established a control environment for properly implementing measures such as verification at the time of transaction.

- A. Whether the BeTI has established internal rules that specify internal arrangements and procedures for implementing measures such as verification at the time of transaction. In addition, whether it has fully communicated the rules to all officers and employees and ensured their full understanding.
  - B. When implementing measures such as verification at the time of transaction, whether the BeTI verifies the credibility and validity of the identity not only by identifying customer attributes such as the birth date and address properly, but also by requiring the submission of customer identification documents, for example. Whether it properly responds to and manages a problem identified in relation to a customer.
  - C. Regarding customer identification data obtained from a customer, whether the BeTI constantly strives to keep track of up-to-date customer attributes through ongoing monitoring of transactions with the customer, for example.
  - D. Whether the BeTI rechecks with respect to the verification implemented at the time of transaction, for example by requiring the re-submission of customer identification documents, when doubt has arisen about the credibility and validity of customer identification data obtained in the past or when it is suspected that a transaction counterparty is impersonating the nominee of the transaction.
  - E. Whether the BeTI takes measures that take account of the specific characteristics of transactions when implementing verification at the time of transaction.
  - F. When hiring officers and employees, whether the BeTI screened candidates from the viewpoint of, at the minimum, properly combating the financing of terrorism and implementing anti-money laundering measures.
  - G. Whether the BeTI provides officers and employees with training and education concerning verification at the time of transaction on a periodic and ongoing basis. Whether it evaluates the level of the understanding of the officers and employees receiving training and takes follow-up measures, when necessary, in light of their implementation of customer identification in daily business processes.
  - H. Whether the BeTI ensures the effectiveness of the verification at the time of transaction by identifying and examining the implementation status of the verification through periodic internal reviews and internal audits, and by revising and reviewing the implementation method, for example.
- (ii) Whether the BeTI has established a control environment for properly implementing the reporting of suspicious transactions.
- A. Whether the BeTI has established internal rules that specify internal arrangements and procedures for the reporting of suspicious transactions. Also, whether it has fully communicated the rules to all officers and employees and ensured their full understanding.

- B. Whether the BeTI ensures that the supervisory department reports to the authorities promptly when a certain transaction is judged to constitute a suspicious transaction.
- C. In judging whether a certain transaction constitutes a case requiring the reporting of suspicious transactions, whether the BeTI judges the necessity of the reporting under Article 8(2) of the Anti-Criminal Proceeds Act and Articles 26 and 27 of the Regulation for Enforcement of the Act on Prevention of Transfer of Criminal Proceeds by comprehensively taking account of the various specific information that it holds with regard to the relevant transaction, such as customer identification data and the circumstances at the time of the transaction. Whether the BeTI responds to and manages any problem identified in relation to the relevant transaction.
- D. When judging whether a certain transaction constitutes a case of suspicious transaction, whether the BeTI takes account of the contents of its own business and customer attributes.
- E. When hiring officers and employees, whether the BeTI screens candidates from the viewpoint of, at the minimum, properly combating the financing of terrorism and implementing anti-money laundering measures.
- F. Whether the BeTI provides officers and employees with training and education concerning the reporting of suspicious transactions on a periodic and ongoing basis. In addition, whether the BeTI evaluates the level of understanding of the officers and employees receiving training and takes follow-up measures when necessary in light of their implementation of reporting in daily business processes.
- G. Whether the BeTI ensures the effectiveness of the reporting of suspicious transactions by identifying and examining the implementation status of the reporting through periodic internal reviews and internal audits, and by reviewing and revising the implementation method, for example.
- (iii) Whether the BeTI has established an integrated and centralized internal control environment for judging whether to implement the reporting of suspicious transactions, by comprehensively taking account of basic customer information obtained through appropriate implementation of verification at the time of transaction, the specific characteristics of transactions and other matters based on the full recognition of the relation between verification at the time of transaction and the reporting of suspicious transactions.
- (iv) Whether the BeTI has developed a control environment to properly implement measures stipulated in the “Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism” (hereinafter referred to as the “AML/CFT Guideline”).
- (Note) Risk-based approach means to identify and assess the risks of money laundering and

financing of terrorism to which one is exposed and take appropriate measures that are complementary with the risks to mitigate them effectively.

### **(3) Supervisory Method and Actions**

With regard to matters pointed out in inspections and issues of supervisory concern regarding verification at the time of transaction, reporting of suspicious transactions and measures stipulated in the AML/CFT Guideline recognized through daily supervisory administration, the supervisory departments must identify and keep track of the status of voluntary improvement made by the BeTI by holding in-depth hearings and, when necessary, requiring the submission of reports based on Article 20(1) of the Book-Entry Transfer Act. When the BeTI is deemed to be at risk of continuing to be used for organized crime by anti-social forces, terrorists, etc. because its internal control environment is extremely fragile, supervisory departments shall take actions, such as issuing an order for business improvement based on Article 21 of the Book-Entry Transfer Act.

In cases where the BeTI is deemed to have committed a serious violation of law, including cases where it has significantly undermined the public interest by violating the obligation for implementing verification at the time of transaction or for reporting suspicious transactions, the authorities shall consider such actions as issuing an order for business suspension based on Article 22(1) of the Book-Entry Transfer Act.

(Note) With regard to verification at the time of transaction, it should be kept in mind that necessary measures may be taken separately as necessary based on the Anti-Criminal Proceeds Act.

## **V-3-2 Business Continuity Management (BCM)**

### **(1) Background and Objectives**

BeTIs function as the core of the securities settlement system through recording and managing transfer account books with special legal effects. They are required to take such actions as formulating an appropriate business continuity plan (BCP) in order to recover their operations as soon as possible and continue their operations even in the event of an emergency, e.g., acts of terrorism, large-scale disasters.

### **(2) Major Supervisory Viewpoints**

(i) Whether the BeTI recognizes what constitutes an emergency and is striving as much as possible to prevent or guard against any emergency by, for example, conducting inspections and anti-crisis practices periodically in normal times.

- (ii) Whether the BeTI formulates emergency response policies, etc., including a BCP, to recover their operations as soon as possible and continue their operations even in the event of an emergency, and periodically reviews them. In particular, whether the BeTI clarifies its decision-making system in crises.
- (iii) Whether the board of directors clearly defines the roles and responsibilities for addressing an emergency and endorses the BeTI's operational risk-management framework in the case of formulating and significantly changing the emergency response policies, etc.
- (iv) Whether the BCP, etc. aims to resume the operation of the indispensable information system within two hours from system halt and to complete settlement on the same day on which the fault occurred.
- (v) Whether the BeTI has developed a control environment for promptly making a report to the Financial Markets Division of the Policy and Markets Bureau of the FSA and making relevant organizations within the BeTI work closely with each other if an emergency has arisen or if the possibility of an emergency has been recognized.
- (vi) Whether the BeTI has established a backup center while taking geographic factors into account as a safety measure to prepare against emergencies. Whether the BeTI backs up business data in a timely manner and periodically conducts drills such as switching over to the backup center.
- (vii) Whether the BeTI has considered measures assuming the possibility of electricity supply, communication lines, public transport and other social infrastructures coming to a halt.

### **(3) Supervisory Method and Actions**

When supervisory departments have recognized an issue of supervisory concern regarding a BeTI's control environment for crisis management, through daily supervisory administration, etc., they shall identify and keep track of the status of voluntary improvement made by the BeTI by holding in-depth hearings and, when necessary, requiring the submission of reports based on Article 20(1) of the Book-Entry Transfer Act.

When supervisory departments have recognized the occurrence of an emergency or the likelihood of an emergency occurring, they shall hold hearings periodically and check the situation first-hand so that they can identify and keep track of how the relevant BeTI is responding to the emergency, including whether the response (status of the development of a control environment for crisis management, securement of book-entry transfer functions, communications with relevant parties, including AMIs, dissemination of information, etc.) is sufficient in light of the level and type of the emergency, until the situation improves. In

addition, they shall require the submission of a report based on Article 20(1) of the Book-Entry Transfer Act when necessary.

### **V-3-3 Operational Risk Management**

#### **(1) Background and Objectives**

Operational Risk is the risk of BeTIs, etc. incurring losses due to their officers and employees failing to conduct administrative work properly, causing accidents or committing illegal acts in the course of the administrative work process, and is deemed to be caused by various factors such as information systems and internal procedures, in addition to human errors.

It is important that BeTIs pursue sound and appropriate business operations by establishing arrangements and procedures for managing operational risks.

#### **(2) Major Supervisory Viewpoints**

- (i) Whether the BeTI has established appropriate policies, procedures, etc. to identify and manage operational risks. Whether the BeTI examines them periodically, and reviews them as necessary. Whether the board of directors endorses such policies, procedures, etc., and clearly defines the roles and responsibilities for addressing operational risk. Also, whether the BeTI has implemented specific measures to reduce operational risks.
- (ii) Whether the BeTI has sufficient processing capacity to achieve a certain level of service in consideration of the volume of administrative processes, etc. expected in the future.
- (iii) In cases where the BeTI outsources part of its administrative processes to service providers or other third parties or relies on them, whether the BeTI confirms that the outsource fulfills the requirements that would have to be met if such processes were carried out by the BeTI itself.
- (iv) Whether the BeTI has specified a policy and procedures for selecting the business operations to be outsourced and the contractors to outsource them to, and concluded a contract and developed a control environment that enables sufficient management of such contractors.

#### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the response by the BeTI, the supervisory departments shall monitor voluntary business improvement made by the BeTI, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 20 of the Book-Entry

Transfer Act.

Furthermore, the supervisory departments shall take actions such as issuing an order for business improvement based on Article 21 of the Book-Entry Transfer Act, when the BeTI's control environment for managing operational risks is deemed to have a serious problem and the action is deemed to be necessary from the viewpoint of properly and reliably conducting book-entry transfer operations.

#### **V-3-4 Information Technology Risk Management**

##### **(1) Background and Objectives**

Information technology risk is the risk that BeTIs, etc. will incur losses generally because of a computer system breakdown, malfunction or other inadequacies, or because of inappropriate or illegal use of computer systems.

BeTIs' systems are themselves market infrastructures that are indispensable for book entry and transfer, etc., so if any system troubles or cybersecurity incidents occur, they may inflict damage on BeTIs and AMIs connected to the systems, and in turn, impact the financial system as a whole.

Therefore, it is important to build a robust control environment for managing information technology risks in BeTIs.

(Note) "Cybersecurity incidents" refers to instances of cybersecurity being threatened by so-called cyberattacks, including unauthorized intrusion, theft, modification and destruction of data, failure or malfunction of information systems, execution of illegal computer programs and DDoS attacks, committed via the Internet through malicious use of information communication networks and information systems.

##### **(2) Major Supervisory Viewpoints**

###### **(i) Recognition of Information Technology Risk**

- A. Whether the board of directors has formulated a basic policy for organization-wide management of information technology risk based on a full recognition of information technology risk.
- B. Whether the board of directors recognizes that prevention and efforts for speedy recovery from system troubles and cybersecurity incidents (hereinafter referred to as "system trouble, etc.") is an important issue and has developed an appropriate control environment.
- C. Whether there are arrangements and procedures for ensuring that information regarding information technology risk is properly reported to the management team.

**(ii) Establishment of Appropriate Control Environment for Risk Management**

- A. Whether the BeTI has specified a basic policy for the management of information technology risk and developed a relevant control environment.
- B. Whether the BeTI has designated the types of risk that should be managed according to specific criteria and has identified the location of the risk.
- C. Whether the control environment for managing information technology risk is effective enough to, enable the BeTI to identify and analyze the actual state of its business operations and system troubles, and minimize the frequency and scale of system troubles in a manner suited to the system environment and other factors, thereby maintaining an appropriate level of computer system quality.

**(iii) Assessment of information technology risk**

Whether the division managing information technology risk recognizes and assesses risks periodically or in a timely manner by recognizing the fact that risks are becoming diversified due to changes in the external environment, such as seen in the examples of system troubles induced by large-scale transactions as a result of increased customer channels and efforts to enhance information networks that bring more diverse and broad-based impact.

Also, whether it is taking sufficient measures to address the risks that have been identified.

**(iv) Management of information security**

A. Whether the BeTI has developed a policy to appropriately manage information assets, prepared organizational readiness, introduced in-house rules, etc., and developed an internal control environment. Also, whether it is making continuous efforts to improve its information security control environment through the PDCA cycle, taking notice of illegal incidents or lapses at other companies.

B. Whether the BeTI is managing information security by designating individuals responsible for it and clarifying their roles/responsibilities in efforts to maintain the confidentiality, integrity and availability of information. Also, whether the individuals responsible for information security are tasked to handle the security of system, data and network management.

C. Whether the BeTI is taking measures to prevent unauthorized use of computer systems, unauthorized access, and intrusion by malicious computer programs such as computer viruses.

D. Whether the BeTI identifies important information of AMIs it is responsible for protecting in a comprehensive manner, keeps its records and manages them.

Whether the BeTI, in identifying important information of AMIs, has set business



operations, systems and external contractors as the scope of protection and includes data, such as listed below, in the scope where it tries to identify those calling for protection.

- Data stored in the areas within the system that are not used in ordinary operations
- Data output from the system for analyzing system troubles, etc.

E. Whether the BeTI is assessing importance and risks regarding important information of AMIs that has been identified.

Also, whether it has developed rules to manage information, such as those listed below, in accordance with the importance and risks of each piece.

- Rules to encrypt or mask information
- Rules for utilizing information
- Rules on handling data storage media, etc.

F. Whether the BeTI has introduced measures to discourage or prevent unauthorized access, unauthorized retrieval, data leakage, etc. such as listed below, for important information of AMIs.

- Provision of access authorizations that limits access to the scope necessary for the person's responsibility
- Storage and monitoring of access logs
- Introduction of mutual checking functions such as by separating the individuals in charge of development and those responsible for operations, administrators and those responsible for operations, etc.

G. Whether the BeTI has introduced rules for controlling confidential information, such as encryption and masking. Also, whether it has introduced rules regarding the management of encryption programs, encryption keys, and design specifications for encryption programs.

Note that "confidential information" refers to information, such as PIN, passwords, etc., whose misuse could lead to losses by AMIs.

H. Whether the BeTI gives due consideration to the necessity of holding/dispersing of, restricting access to, and taking outside, of confidential information, and treats such information in a stricter manner.

I. Whether the BeTI periodically monitors its information assets to see whether they are managed properly according to management rules, etc. and reviews the control environment on an ongoing basis.

J. Whether the BeTI conducts security education (including by external contractors) to all officers and employees in order to raise awareness of information security.

**(v) Management of cybersecurity**

A. Whether the board of directors, etc. recognizes the importance of cybersecurity amid increasingly sophisticated and cunning cyberattacks and has introduced the necessary control environment.

B. Whether the BeTI has introduced systems to maintain cybersecurity, such as listed below, in addition to making the organization more secure and introducing in-house rules.

- Monitoring systems against cyberattacks

- Systems to report cyberattacks and public-relation systems when attacks occur

- Emergency measures by Computer Security Incident Response Teams and systems for early detection

- Systems of information collection and sharing through information-sharing organizations, etc.

C. Whether the BeTI has introduced a multi-layered defence system against cyberattacks that combines security measures respectively for inbound perimeter control, internal network security control and outbound perimeter control.

- Security measures for inbound perimeter control (e.g. introduction of a firewall, anti-virus software, Intrusion Detection System, Intrusion Protection System etc.)

- Security measures for internal network security control (e.g. proper management of privileged IDs/passwords, deletion of unnecessary IDs, monitoring of execution of certain commands, etc.)

- Security measures for outbound perimeter control (e.g. retrieval and analysis of communication/event logs, detecting/blocking inappropriate communication, etc.)

D. Whether measures such as listed below are implemented to prevent damage from expanding when cyberattacks occur.

- Identification of IP addresses from which the cyberattacks originate and blocking off of attacks

- Functions to automatically spread out accesses when under DDoS attacks

- Suspension of the entire system or its part, etc.

E. Whether necessary measures for vulnerabilities in the system, such as updating of the operating system and application of security patches, are introduced in a timely manner.

F. Whether the BeTI is, as part of cybersecurity measures, assessing its security levels by taking advantage of tests on network intrusion, vulnerability scanning or penetration tests, etc. and making efforts to improve security.

G. Whether the BeTI, when carrying out business operations using communication methods such as the Internet, has introduced appropriate authentication methods in

line with the risks associated with such transactions, such as listed below.

-Authentication methods that do not rely on fixed IDs or passwords, such as variable passwords and digital certificates

-Transaction authentication using transaction signatures by means of a hardware token, etc.

H. Whether the BeTI, when carrying out business operations using communication methods such as the Internet, has introduced preventative measures in line with operations, such as listed below.

-Introduction of software that allows the BeTI to detect the state of virus infection of the AMI's PC and issue a warning

-Adoption of methods to store digital certificates in mediums or devices separate from the PCs used in the relevant business operation, such as IC cards

-Introduction of a system that allows the BeTI to detect unauthorized log-ins, abnormal input, etc. and immediately notify such abnormalities to AMIs

I. Whether the BeTI has developed contingency plans against potential cyberattacks, conducts exercises and reviews such plans. Also, whether it participates in industry-wide exercises as necessary.

J. Whether the BeTI has formulated plans to train and expand the personnel responsible for cybersecurity and implements them.

**(vi) System Planning, Development and Operational Management**

A. Whether the BeTI has formulated a medium/long-term development plan after having clarified its strategic policy for systems as part of its management strategy. Whether the medium/long-term development plan has been approved by the board of directors.

B. Whether the BeTI reveals the risks inherent to its existing systems on an ongoing basis, and makes investments to maintain and improve the systems in a planned manner.

C. Whether the BeTI has clarified its rules for approval of plans, development and transition in development projects.

D. Whether the BeTI specifies the responsible person with respect to each development project and manages the progress based on the development plan.

E. Upon system development, whether the BeTI conducts tests in an appropriate and sufficient manner, such as by preparing test plans and making user divisions participate.

F. For human resources development, whether the BeTI formulates and implements specific plans to pass on the mechanism and development technologies of its existing systems and train personnel with expertise.

**(vii) Computer System Audits**

- A. Whether an internal audit section that is independent from the computer system division and has auditing staff adept in computer systems conduct periodic audits of the computer system.
- B. Whether the BeTI conducts internal audits by subject matter about computer systems and is taking of external audits by information system auditors.
- C. Whether the audited division accounts for all business operations involving information technology risk.

**(viii) Management of Outsourcing of Business Operations**

- A. Whether the BeTI selects outsourcees (including system subsidiaries) by evaluating and examining them based on selection criteria.
- B. Whether the BeTI has prescribed the allocation of roles and responsibilities, audit authority, subcontracting procedures, level of services rendered, etc. with the outsource in an outsourcing agreement. Also whether the BeTI presents to outsourced contractors rules and security requirements their employees are required to adhere to and security requirements, as well as defines them in contract forms, etc.
- C. Whether the BeTI properly conducts risk management regarding outsourced business operations (including work further subcontracted) related to the computer system. In cases where system-related administrative processes are outsourced, whether the BeTI properly conducts risk management according to the outsourced business operations related to the computer system.
- D. Whether the BeTI periodically monitors the outsourced business operations (including work further subcontracted) to determine, as the outsourcer, that the outsourced business operations are properly conducted.

Also, whether there is a system that allows the consigner to monitor and track the status of data of investors and AMIs being processed at outsourced contractors.

**(ix) Contingency Plan**

- A. Whether the BeTI has formulated a contingency plan and has established arrangements and procedures for dealing with emergencies.
- B. Whether the BeTI is basing the details of its contingency plan on guides that allows it to judge objective levels of its details (such as “Guide to Formulate Contingency Plans at Financial Institutions” compiled by the Center for Financial Industry Information Systems).
- C. Whether the BeTI, in developing a contingency plan, assumes not only contingencies due to natural disasters but also system troubles, etc. due to internal or external factors.

Also, whether it assumes risk scenarios of sufficient extent for cases such as a major delay in batch processing.

- D. Whether the BeTI reviews assumed scenarios in its contingency plan by, for example, taking into consideration case studies of system troubles, etc. at other financial institutions, clearing organizations, fund clearing organizations, book-entry transfer institutions and trade repositories, and the results of deliberations at the Central Disaster Management Council, etc.
- E. Whether exercises in accordance with the contingency plan involve the entire company and are periodically conducted jointly with outsourced contractors, etc.
- F. Whether off-site backup systems, etc. are introduced for important systems whose failure could seriously affect business operations, and that a control environment is in place to address disasters, system troubles, etc. so that normal business operations can be speedily brought back.

**(x) Risk of System Updates, etc.**

- A. Whether the BeTI has developed a control environment for managing the risk of system updates, etc. by ensuring that its officers and employees fully recognize the risk.
- B. Whether the BeTI has established arrangements and procedures for conducting tests. Whether its test plan is suited to the nature of the system development necessitated by the system updates, etc.
- C. Whether the BeTI has established a control environment that enables itself to be proactively involved in the system updates, etc. when this task is outsourced.
- D. Whether the BeTI makes use of third-party evaluation, such as evaluation by a system auditor, when making judgment regarding important matters related to the system updates, etc.
- E. Whether the BeTI has developed a contingency plan for dealing with an unexpected incident.

**(xi) Response to System Troubles**

- A. Whether the BeTI implements appropriate measures to avoid creating unnecessary confusion among investors, AMIs, etc. when system troubles, etc. occur and performs tasks towards the prompt recovery and operation of alternatives.  
Also, whether it has developed a worst-case scenario in preparation for system troubles and is prepared to take necessary measures accordingly.
- B. Whether the BeTI has prepared procedures that also subjects outsourced contractors to reporting system troubles, and has a clearly defined system of command and supervision.

C. Whether the BeTI is prepared to immediately notify the representative director and other directors when a system trouble that may significantly affect business operations occurs, and report the largest potential risk it poses under the worst-case scenario (for example, if there is a possibility that the failure could gravely affect investors or AMIs, etc., the reporting persons should not underestimate the risk but immediately report the biggest risk scenario).

In addition, whether it is prepared to launch a task force, have the representative director issue appropriate instructions and orders, and seek resolution of the issue in a swift manner.

D. Whether the BeTI, after system troubles, etc. have occurred, analyzes the cause and implements measures based on the analysis to prevent recurrence.

Also, whether it periodically analyzes tendencies of factors that have led to system troubles, etc. and introduces measures to address them.

E. Whether the BeTI immediately reports system troubles, etc. to the authorities.

### **(3) Supervisory Method and Actions**

#### **(i) At the Time of Problem Recognition**

When supervisory departments have recognized an issue of supervisory concern regarding a BeTI's control environment for managing information technology risk, through daily supervisory administration, etc., they shall identify and keep track of the status of voluntary improvement made by the BeTI, by holding in-depth hearings with the BeTI and the outsourcing contractor and, when necessary, requiring the submission of reports based on Article 20(1) of the Book-Entry Transfer Act.

When the BeTI is deemed to have a serious problem from the viewpoint of properly and reliably conducting book-entry transfer operations, the supervisory departments shall take actions, such as issuing an order for business improvement, etc., based on Article 21 of the Book-Entry Transfer Act.

#### **(ii) At the Time of System Updates, etc.**

In cases where BeTIs are to perform system updates, etc., they shall be required to submit specific plans for implementing the system updates, etc. and documents regarding the internal control environment for managing the risk associated with the system updates, etc. (including internal audits) and other matters according to their characteristics.

In cases where the system updates, etc. are large in scale, BeTIs shall be required to periodically submit reports based on Article 20(1) of the Book-Entry Transfer Act until such system updates, etc. are completed.

#### **(4) Response to System Troubles**

- (i) BeTIs shall be required to notify the authorities of the occurrence of any computer system troubles as soon as they have recognized it, and submit a “Report on Problem Occurrence, etc.” (in the format specified in Attached List of Formats 3-1) to the authorities.

After the computer system operation has been restored to normal and the cause of the problem has been identified, they shall be required to report to the authorities again. (It should be kept in mind that they shall be required to report to the authorities on the current state within one month even if the computer system operation has not been restored to normal or the cause of the problem has not been identified within the one-month period.)

(Note) Computer System Trouble Subject to Reporting to the Authorities

Problems that must be reported to the authorities are those which affect systems and equipment (including both hardware and software) used by BeTIs and contractors undertaking business operations outsourced by BeTIs, and which could affect the BeTIs’ abilities to identify and keep track of the status of transactions, financial settlements, cash deposits and withdrawals, fund-raising and financial conditions, and undermine the convenience of AMIs, etc. in other ways.

However, the reporting requirement is not applicable to such system troubles in cases where a backup system has started up and effectively prevented adverse effects.

It should be noted that even if no computer system troubles have occurred, a report must be made in cases where AMIs or business operations will be affected or are highly likely to be affected, including cases where a BeTI has received a warning of a cyber attack on its computer system or where it has detected the possibility of such an attack.

- (ii) A BeTI who has reported computer system troubles to the authorities shall be required to submit an additional report based on Article 20(1) of the Book-Entry Transfer Act when necessary. When the BeTI is deemed to have a serious problem from the viewpoint of properly and reliably conducting book-entry transfer operations, the authorities shall take actions, such as issuing an order for business improvement based on Article 21 of the Book-Entry Transfer Act.

When the BeTI is deemed to have committed a serious and malicious violation of law, the authorities shall consider necessary actions, including the issuance of an order for business suspension based on Article 22(1) of the Book-Entry Transfer Act.

## **V-3-5 Procedures to Deal with Default of AMIs, etc.**

### **(1) Background and Objectives**

In the event of default, etc. of AMIs, BeTIs need to promptly take actions, such as implementing administrative procedures from the viewpoint of continuing to facilitate book-entry transfer operations and ensuring facilitation of circulation of securities.

From this perspective, BeTIs are required to clearly establish administrative procedures to be taken by BeTIs and AMIs to deal with default, etc. BeTIs also need to properly verify whether such procedures are actually executable in practice in the event of default, etc. of AMIs.

### **(2) Major Supervisory Viewpoints**

- (i) Whether the BeTI has clearly established procedures in its Business rules with respect to the default, etc. of an account management institution, in order to enable the continuation of smooth business operations such as book-entry transfer operations of the BeTI.
- (ii) Also, whether the BeTI tests periodically, at least once a year, and reviews as necessary, the procedures to deal with the default, etc. of AMIs in collaboration with AMIs and other parties concerned.
- (iii) Whether the BeTI has developed a manual, etc. to deal with the default, etc. of AMIs and periodically verifies its feasibility with employees involved in the procedures to deal with the default, etc. of AMIs as well as with AMIs and other parties concerned.
- (iv) Whether the BeTI has established clear rules and procedures to smoothly implement administrative procedures even in the event of individual or combined default, etc. among AMIs.

### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the procedures to deal with the default, etc. of AMIs, the supervisory departments shall monitor voluntary business improvement made by the BeTI, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 20(1) of the Book-Entry Transfer Act.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 21 of the Book-Entry Transfer Act when it is deemed necessary to do so from the viewpoint of properly and reliably conducting book-entry transfer operations.



### **V-3-6 Notes concerning Tiered Structure of Participants, etc.**

#### **(1) Background and Objectives**

With regard to the use of BeTIs, there are tiered participation arrangements under which an AMIs has another participant that opens accounts with the AMIs and by this way participates in a BeTI's book entry and transfer systems. Such tiered participation arrangements enable many subordinate account management institutions to use the book-entry transfer system through senior account management institutions, while the business structure might become complicated depending on the relationship between the senior and subordinate account management institutions and the nature of the business process, giving rise to various potential risks. BeTIs need to identify risks inherent to such tiered participation arrangements and establish appropriate arrangements and procedures for managing such risks.

#### **(2) Major Supervisory Viewpoints**

- (i) Whether the BeTI identifies risks involved in tiered participation arrangements and takes measures to manage such risks in its rules, procedures, etc., such as gathering basic information about the tiered structure.
- (ii) Whether the BeTI examines the risks with respect to AMIs which have a very large number of participants, identified by gathering information as referred to above or by other means.

#### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the arrangements and procedures for managing risks arising from tiered participation arrangements, etc., the supervisory departments shall monitor voluntary business improvement made by the BeTI, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 20(1) of the Book-Entry Transfer Act.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 21 of the Book-Entry Transfer Act when it is deemed necessary to do so from the viewpoint of properly and reliably conducting book-entry transfer operations.

### **V-3-7 Appropriateness of Disclosure of Information, etc.**

### **(1) Background and Objectives**

It is important that BeTIs provide sufficient information so that AMIs and prospective AMIs can clearly recognize and fully understand the risks and responsibilities arising from their participation in the book-entry transfer system.

Furthermore, from the viewpoint of providing sufficient information to users, etc., it is important that key procedures concerning the rights and obligations of users, etc. are clarified and publicly disclosed in business rules and other rules and procedures.

### **(2) Major Supervisory Viewpoints**

(i) Whether the BeTI has formulated clear and comprehensive rules and procedures and disclosed them to AMIs. Whether the BeTI publicly discloses key rules, procedures, etc.

(ii) In the aforementioned rules, procedures, etc., whether the BeTI clearly describes the rights and obligations of the BeTI and AMIs.

(iii) Whether the BeTI clarifies operations performed at a charge and operations performed without charge, and publicly discloses the fee and content of individual services.

(iv) Whether the BeTI periodically discloses information based on the “Principles for Financial Market Infrastructures” and the “Disclosure framework and Assessment methodology”<sup>(Note)</sup> that supplements the principles.

(Note) CPSS and IOSCO, “Disclosure framework and Assessment methodology” (December 2012)

### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the disclosure of major rules, etc. by the BeTI, the supervisory departments shall monitor voluntary business improvement made by the BeTI, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 20(1) of the Book-Entry Transfer Act.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 21 of the Book-Entry Transfer Act when it is deemed necessary to do so from the viewpoint of properly and reliably conducting book-entry transfer operations.

## **V-4 Administrative Procedures**

### **V-4-1 Points to Consider regarding Authorization of Business Rules, etc.**

#### **(1) Background and Objectives**

Business rules prescribe the desirable status of business operations of a BeTI as well as basic matters regarding the BeTI's book-entry transfer system, such as obligations of BeTIs and AMIs, measures that may be taken by BeTIs, contracts between AMIs and participants, assuming authorization by the authorities.

In light of the above, BeTIs are required to clearly establish rules and procedures, etc. for business rules and clarify their basis and characteristics so that financial transactions can be handled by AMIs, etc. in a smooth, continuous and stable manner.

#### **(2) Major Supervisory Viewpoints**

- (i) When making amendments, etc. to business rules, whether the BeTI confirms that the book-entry transfer system as a whole, including business rules and subordinate rules, etc. is consistent with laws and regulations, etc.
- (ii) Whether the BeTI discloses and as necessary explains such amendment, etc. to AMIs, etc. in a clear and easy-to-understand manner at least after receiving authorization by the authorities, or as necessary, before then.
- (iii) When giving such explanation, whether the BeTI summarizes the basis and applicability of laws and regulations pertaining to contracts on book-entry transfer, etc.
- (iv) In cases where there is a foreign account management institution, whether the BeTI confirms the risks associated with differences in laws and regulations, including confirming the laws and regulations, etc. of the country concerned.
- (v) When confirming and explaining the above, whether the BeTI gives consideration to the accuracy of such confirmation and explanation by such means as utilizing outside experts as necessary.
- (vi) In the rules for business rules, etc., whether the BeTI has clarified the point at which settlement is final in its rules and procedures.
- (vii) Whether the BeTI confirms that the provisions on the above are consistent with laws and regulations, etc. and explains them as necessary to AMIs, etc.

### **V-4-2 Points to Consider regarding Approval of Subsidiary Business**

#### **(1) Purpose**

BeTIs' activities may directly affect ordinary investors' interests as they are responsible for the recording and management of transfer account books with special legal effects. Therefore, they are strongly required to maintain their financial soundness and conduct business operations in a stable manner.

Considering their highly public nature as such, BeTIs must concentrate on book-entry transfer operations, and in principle, are not able to conduct any other business, for the purpose of blocking out risks from operations other than their core business (Article 9(1) of the Book-Entry Transfer Act).

On the other hand, based on the view that the provision of services other than their primary business may help improve convenience, stability, etc. of the settlement system as a whole in light of users' needs, even if they do not correspond to book-entry transfer operations, BeTIs are able to conduct business related to book-entry transfer operations that is found to have no risk of hindering their properly and reliably conducting of book-entry transfer operations, as related business, by obtaining approval.

## **(2) Application for Approval**

Upon making an application for approval, the BeTI shall submit the approval application form prescribed in Article 6(1) etc. of the Order on Supervision of General Book-entry Transfer Institutions (Attached List of Formats 3-2) and the attached documents listed in the items of Article 6(2) of said Order.

## **(3) Approval Screening**

Upon approval screening, it is necessary to determine the appropriateness of approval on a case-by-case basis, in view of such matters as whether there is a risk of hindering the BeTI from properly and reliably conducting book-entry transfer operations. Specifically, approval screening shall be conducted from the following viewpoints.

- (i) Whether there is a high likelihood of causing losses for the BeTI and affecting its management.
- (ii) Whether the BeTI has identified the risks to which it will be exposed and has established arrangements and procedures for managing such risks properly.
- (iii) Whether there is a risk of undermining confidence in the fairness and impartiality of the book-entry transfer operations or undermining the social credibility as a BeTI.
- (iv) Whether the workload hinders the appropriate implementation of the book-entry transfer operations.
- (v) Whether the business, in light of its content and characteristics, helps the smooth implementation of the book-entry transfer operations. Whether the business helps

facilitate the circulation of corporate bonds, etc. through increasing in convenience for AMIs.

**(4) Supervisory Method and Actions after Granting Approval**

BeTIs are important social infrastructures that ensure speedy and reliable means of settlement, and authorities are required to conduct monitoring on an ongoing basis so that the sound and appropriate operation of their primary business is not hindered due to other business operations, say, as a result of the confidence in BeTIs being undermined.

In cases where other business conducted by a BeTI is hindering or has the risk of hindering the sound and appropriate operation of its primary business, the supervisory departments shall monitor voluntary business improvement made by the BeTI, by holding an in-depth hearing and, when necessary, requiring the submission of a report based on Article 20(1) of the Book-Entry Transfer Act.

Furthermore, the supervisory departments shall consider taking actions such as issuing an order for business improvement under the provision of Article 21 of the Book-Entry Transfer Act when it is deemed necessary to do so from the viewpoint of properly and reliably conducting book-entry transfer operations.

## **VI. Supervisory Viewpoints and Procedures (Trade Repositories)**

### **VI-1 Governance / Business Administration**

#### **VI-1-1 Governance System**

##### **(1) Background and Objectives**

TRs play an important role in improving the transparency of transaction information by intensively managing transaction data in the over-the counter derivatives market. Under these circumstances, there shall be effective disciplines for management and proper governance in TRs, in order to ensure appropriate business operations and sound management of TRs, and in turn, financial system stability.

Effective functioning of governance presumes that the components of the organization are fulfilling their primary roles. Specifically, it is important that, for example, organs such as the board of directors and the board of auditors are able to check management, and checks and balances among divisions are functioning properly, as is the internal audit section. It is also necessary for representative directors, directors, executive officers, auditors and employees in all positions to understand their respective roles and be fully involved in the process.

(Note) Under the FIEA, TRs may be established either as a company with a board of auditors or as a company or other juridical person (including an organization which is not a juridical person and for which there is a provision for the appointment of a representative, etc. Therefore, in the case of TRs which are not companies with a board of auditors, it is necessary to examine whether their representatives, managers, committees, etc. are properly exercising their respective authority. The examination should be conducted with due consideration of the actual status of management based on the purpose of these Guidelines.

##### **(2) Major Supervisory Viewpoints**

###### **[Representative Director]**

- (i) Whether the representative director considers compliance as one of the important management issues and takes the initiative in building a control environment for compliance.
- (ii) Whether the representative director fully recognizes that disregarding the risk management division may have a serious impact on corporate earnings and attaches importance to the said division.

### **[Directors/Board of Directors]**

- (i) Whether directors check and prevent autocratic management by the representative director and other officers who are responsible for business execution, and are actively involved in the board of directors' decision-making and checking process concerning business execution.
- (ii) In cases where outside directors are appointed, whether they recognize their own significance from the viewpoint of ensuring objectivity in the decision-making of management, etc. and proactively participate in the meetings of the board of directors. In cases where proposals for the appointment of outside directors are to be determined, whether the outside directors' personal relationships and equity relationships with the TR and other interests are verified and their independence, aptitude, etc. are carefully examined, in consideration of the roles they are expected to fulfill. Whether some kind of framework has been established so that outside directors would make appropriate judgments at the meetings of the board of directors; for example, whether information is provided on an ongoing basis.
- (iii) Whether the board of directors takes measures to objectively ensure the appropriateness and fairness of, for example, important management decisions and management judgments related to compliance, etc. such as utilizing the advice of outside experts and discretionary committees whose members consist of outside experts as necessary when making such decisions and judgments. In particular, whether the board of directors takes measures to appropriately reflect **the legitimate interests** of its **users** and other relevant stakeholders on design, rules, overall strategy, and major decisions.
- (iv) Whether the board of directors has specified a management policy based on the overall vision of the desirable status of the TR. Whether it has established management plans in line with the management policy and communicated the plans throughout the organization. Whether it regularly reviews and revises the progress status thereof.
- (v) Whether directors and the board of directors are sincerely leading efforts in compliance and are properly demonstrating the board's functions to establish an organization-wide internal control environment.
- (vi) Whether the board of directors fully recognizes that disregarding the risk management division may have a serious impact on corporate earnings, and attaches importance to the said division. In particular, whether the director in charge has in-depth knowledge and understanding concerning the methods of measuring, monitoring and managing risks, in addition to an understanding of where risks reside and what kind of risks they are.
- (vii) Whether the board of directors has set up a policy for managing risks based on

strategic objectives and communicated it throughout the organization. Whether it reviews the risk management policy on a periodic or as-needed basis. In addition, whether the board of directors makes use of risk-related information in the execution of business and the development of risk management systems by, for example, making necessary decisions based on the status of risks reported periodically.

**[Auditors/Board of Auditors]**

- (i) Whether the independence of the auditors and the board of auditors is ensured in accordance with the purpose of the board of auditors system.
- (ii) Whether the auditors and the board of auditors properly exercise the broad authority granted thereto and conduct audits of business operations in addition to audits of accounting affairs.
- (iii) Whether individual auditors recognize the importance of their own independence within the board of auditors and actively take the initiative to conduct audits.
- (iv) Whether the auditors and the board of auditors strive to ensure the effectiveness of their audits by, for example, receiving reports on the results of external audits, depending on the contents thereof.

**[Internal Audit Section]**

- (i) Whether the internal audit section is independent from divisions subject to audit so as to fully check the actions thereof, has the control environment and ability to collect important information on their operational status, etc. in a timely manner, and is sufficiently staffed and equipped to conduct effective internal audits that are accurately adapted to the environment surrounding the TR and its operational status.
- (ii) Whether the internal audit section formulates efficient and effective internal audit plans that give consideration to frequency and depth according to the type and magnitude of risks based on its understanding of the status of risk management, etc. by divisions subject to audits, properly reviews the plans depending on the situation, and conducts efficient and effective internal audits based on the internal audit plans.
- (iii) Whether the internal audit section reports important issues pointed out in internal audits without any delay to the representative director and the board of directors. Whether the internal audit section has accurately identified the status of improvements made on the issues pointed out.

**[Use of External Audits]**

- (i) Whether external audits are effectively utilized, with sufficient understanding that



effective external audits are indispensable for ensuring sound and appropriate business operations of TRs.

- (ii) Whether external audits are examined periodically as to whether they are effectively functioning, and appropriate measures are taken with respect to the external audit results, etc.
- (iii) Whether such matters as the number of consecutive years of service by a certified public accountant involved are handled properly.

### **(3) Supervisory Method and Actions**

Supervisory departments shall examine the status of governance through the following hearings and daily supervisory administrative processes.

#### **(i) Comprehensive Hearings (See II-1-1 (1))**

Supervisory departments shall hold hearings regarding TRs' management challenges, strategies and the status of risk management and governance, among other matters. In addition, senior supervisory departments shall directly hold hearings with top managers of TRs as necessary.

#### **(ii) Examination of Governance through Daily Supervisory Administrative Processes**

Supervisory departments shall examine the effectiveness of governance not only through the hearings described above but also through daily supervisory administrative processes, such as follow-up on reports on business improvements made on matters pointed out in inspections.

#### **(iii) Recording of Monitoring Results**

Supervisory departments shall compile and store records on matters of particular note based on the results of monitoring conducted through procedures described above, and make effective use thereof in future supervisory administrative processes.

#### **(iv) Supervisory Method and Actions**

In cases where doubt has arisen about the effectiveness of a TR's governance, the supervisory departments shall monitor voluntary business improvement made by the TR, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-80 of the FIEA.

Furthermore, the supervisory departments shall take actions, such as issuing an order for business improvement based on Article 156-81 of the FIEA, when it is deemed necessary and appropriate to do so from the viewpoint of protecting the public interest and investors.

## **VI-1-2 Officers of Trade Repositories**

### **(1) Major Supervisory Viewpoints**

From the viewpoint of maintaining the public nature of trade repository service, supervisory departments shall pay attention to the following points when examining the decision-making process regarding proposals for the appointment of officers of the TR, among others.

- (i) The officer shall neither meet any of the ineligibility criteria (Article 156-67(1)(iv)(a) to (f) of the FIEA) nor have met any of them at the time when the TR obtained a designation.
- (ii) The officer shall neither have violated laws and regulations regarding trade repositories operations or business incidental thereto nor have breached any administrative actions taken based on laws and regulations.
- (iii) The officer shall not have engaged in an illegal or markedly inappropriate act regarding trade repository services under particularly grave circumstances.

### **(2) Supervisory Method and Actions**

Supervisory departments shall consider taking actions, such as ordering the dismissal of an officer of a TR under the provision of Article 156-83(1) of the FIEA when said officer: (i) meets any criteria specified in Article 156-67(1)(iv)(a) to (f) of the FIEA, or is found to have already met such criteria at the time when the TR obtained a license or approval; (ii) is found to have become an officer of the TR by fraudulent means; or (iii) violates or is found to have violated laws and regulations or administrative actions taken based on laws and regulations.

In addition, they shall hold an in-depth hearing regarding the decision-making process concerning the proposal for the appointment of the said officer or committee member and, when necessary, require the submission of a report based on Article 156-80 of the FIEA. Furthermore, supervisory departments shall consider taking actions, such as issuing an order for business improvement (Article 156-81 of the FIEA), if the TR's control environment for governance is deemed to have a serious problem and the action is deemed to be necessary and appropriate, from the viewpoint of protecting public interest and investors.

## **VI-1-3 Staffing**

### **(1) Major Supervisory Viewpoints**

Supervisory departments shall examine whether TRs are adequately staffed to properly and reliably conduct financial instruments obligation assumption service, in light of the following requirements regarding TRs' officers and employees.

- (i) Whether the TRs have secured officers and employees who understand the viewpoints regarding governance that are specified under the FIEA and other relevant regulations, as well as these Guidelines, and who have the knowledge and experience necessary for conducting governance as well as sufficient knowledge and experience concerning the control environment for compliance required to properly and reliably execute the trade repository services.
- (ii) Whether officers or employees are current or former members of organized crime groups or have a close relationship with organized crime groups.
- (iii) Whether officers or employees have the experience of being sentenced to a fine (including similar punishments imposed under foreign laws and regulations equivalent thereto) for violation of the FIEA or other domestic financial laws and regulations or foreign laws and regulations equivalent thereto.
- (iv) Whether officers or employees have the experience of being sentenced to a fine (including similar punishments imposed under foreign laws and regulations equivalent thereto) for violation of the Act on Prevention of Unjust Acts by Organized Crime Group Members (excluding the provisions of Article 32-3(7) and Article 32-11(1) of said Act) or other foreign laws and regulations equivalent thereto, or for committing a crime prescribed under the Penal Code or under the Act on Punishment of Physical Violence and Others.
- (v) Whether officers or employees have the experience of being sentenced to imprisonment with work or more severe punishment (including similar punishments imposed under equivalent foreign laws or regulations). In particular, whether officers or employees have been accused of committing crimes specified under Articles 246 to 250 of the Penal Code (fraud, fraud using computers, breach of trust, quasi fraud, and extortion as well as attempts at these crimes).

## **(2) Supervisory Method and Actions**

The requirements specified in (i) to (v) above are part of a comprehensive set of elements that should be taken into consideration when supervisory departments examine whether a TR is adequately staffed to properly and reliably conduct trade repositories operations. Even if an officer or an employee is deemed to not meet the requirements, it should not automatically lead to the conclusion that the TR is not adequately staffed. The important thing is, first and foremost, that TRs strive to ensure on their own responsibility

that they are adequately staffed, in light of those requirements and other elements.

However, supervisory departments shall hold in-depth hearings regarding the TR's awareness of such staffing and the decision-making process concerning the proposed appointments of officers and employees, in cases where a TR is deemed to have failed to take those elements into consideration sufficiently in the said decision-making process, and where it is deemed to be necessary and appropriate to hold such hearings in relation to the business operations of the TR from the viewpoint of protecting the public interest and investors. In addition, they shall require the submission of reports under the provision of Article 156-80 of the FIEA when necessary.

Supervisory departments shall consider taking actions, such as issuing an order for business improvement under Article 156-81 of the FIEA, in cases where the TR's control environment for governance is deemed to have a serious problem as a result of the examination of the submitted report, and where the action is deemed to be necessary and appropriate from the viewpoint of protecting the public interest and investors.

## **VI-2 Financial Soundness**

### **VI-2-1 Adequacy of Capital**

#### **(1) Background and Objectives**

In order for TRs to gain users' and market players' confidence and to operate their business continuously and stably, it is important for TRs to retain a sufficient financial basis according to the characteristics of management as well as to establish appropriate arrangements and procedures for managing operational risks and other such risks.

Accordingly, TRs should hold enough liquid assets to withstand any losses that may be incurred in the event that various risks are actualized.

TRs also need to have a process for evaluating their capital adequacy in the context of their risk profiles, and implement appropriate measures for maintaining a sufficient level of capital.

#### **(2) Major Supervisory Viewpoints**

##### **[Directors/Board of Directors]**

- (i) Whether the directors have a general understanding of the nature and level of the risks taken by the TR as well as the relationship between risk and the appropriate level of capital.
- (ii) Whether the directors and the board of directors understand that, in order to achieve their strategic objectives, a capital plan, which is consistent with them, is an essential component, and whether they have formulated an appropriate capital plan according to the management issues of the TR.
- (iii) Whether the directors have been sufficiently involved in formulating the aforementioned capital plan, and are adopting a process for evaluating capital adequacy and implementing appropriate measures for maintaining a sufficient level of capital.

##### **[Capital Adequacy]**

- (i) Upon formulating the aforementioned capital plan, whether the TR evaluates the adequacy of capital relative to the risks measured in consideration of changes in the business environment, etc.
- (ii) As for the amount of assets (e.g. the amount of net assets) to be held to prepare against business risks, which should not include financial sources procured for the purpose of preparing against credit risks and liquidity risks incurred in participant default, whether the TR has secured at least six months worth of operating expenditures, and examined

the sufficiency of the level of such amount in consideration of ensuring the TR's business continuity.

- (iii) Whether the TR properly examines equity capital, for example, as to whether the equity capital consists primarily of cash and cash equivalents, etc. and can thus be easily liquidated in a stress scenario.
- (iv) Whether the TR has a feasible plan to raise additional capital if the level of capital approaches or falls below levels that would make its business continuity uncertain.

## **VI-2-2 Risk Management Framework**

### **(1) Background and Objectives**

TRs intensively accumulate information concerning their over-the-counter derivatives transactions provided by users. Therefore, when conducting business operations, they are required to recognize that they face not only operational risks, such as administrative errors and divulging of information, but also various other risks, including information technology risk, comprehensively check whether or not such risks affect its business operations, and establish appropriate arrangements and procedures for managing risks.

### **(2) Major Supervisory Viewpoints**

- (i) Whether the risk management division has sufficient authority, independence, resources, and access to the board in order to conduct effective risk management. For example, whether the reporting lines for risk management are clear and separate from those for other operations of the TR, so that the matters can be directly reported to the board of directors by the authority of the risk management division.
- (ii) Whether the TR has revealed and identified all risks in order to grasp diverse risks in a comprehensive manner, and if possible, has properly determined risk categories to place them under quantitative risk management.
- (iii) Whether the TR reviews the scope of quantification and accuracy to improve them as necessary. For example, whether the TR reviews the importance, correlation, etc. of different types of risks to ensure appropriateness.
- (iv) Whether the board of directors has clearly set up a policy for managing risks based on strategic objectives in accordance with the management policy of the TR as a whole, and examines the policy periodically, at least annually, and revises it as necessary. In addition, whether the board of directors takes appropriate measures to make the risk management policy widely known within the organization.
- (v) Whether the board of directors makes use of risk-related information in the execution of business and the

development of risk management systems by, for example, making necessary decisions based on risk status reports received periodically.

- (vi) Whether the TR takes measures to identify and manage potential sources of risk arising from the set of contractual and operational arrangements among other financial market infrastructures that connect the TR directly or through an intermediary before entering into such arrangements, and on an ongoing basis once such arrangements are established.

### **VI-2-3 Supervisory Method and Actions**

In cases where a problem has been found in the soundness of the financial condition of a TR, the supervisory departments shall monitor voluntary business improvement made by the TR, by holding an in-depth hearing regarding the cause of the problems and improvement measures and, when necessary, requiring the submission of reports Article 156-80 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement based on Article 156-81 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting the public interests and investors.

## **VI-3 Operational Appropriateness**

### **VI-3-1 Compliance**

#### **VI-3-1-1 Measures for Ensuring Compliance**

##### **(1) Notes Regarding Policies, Procedures, etc. Pertaining to Compliance**

- (i) Whether the TR regards compliance as one of the most important issues for management, and whether it has formulated a basic policy concerning the implementation of compliance, as well as a detailed implementation plan (compliance program) and a code of conduct (ethics code, compliance manual), etc.
- (ii) Whether the TR has clearly established the authority and responsibility of the chief compliance officer, and whether there is a system in place for his/her function to be fully exercised.
- (iii) Whether the TR has established a system for communicating and reporting compliance-related information appropriately among the management team, the divisions in charge of the clearing operations, and the compliance division, chief compliance officer or other person in charge.

##### **(2) Notes Regarding the Whistle-blowing System**

- (i) Whether the TR has clearly designated the division in charge of the whistle-blowing system and established specific procedures for handling internal allegations, so as to ensure that they are processed and a response is made in a prompt and appropriate manner.
- (ii) Whether the TR has developed a system wherein information on the content of internal allegations can be shared within a necessary and appropriate scope.
- (iii) Whether the TR makes sure to properly follow up on how internal allegations are being handled.
- (iv) Whether the TR accurately and appropriately records and stores the details of internal allegations and the results of investigations thereof, and whether it makes full use of this information such as to improve its operational control system and to formulate measures for preventing a recurrence.

#### **VI-3-1-2 Fair Access Requirements, etc.**

##### **(1) Background and Objectives**



Given the role of TRs, which is to contribute to the efficient business operations of users by intensively accumulating and storing information concerning over-the-counter derivative transactions, TRs' services should be fair and open to users.

At the same time, TRs are required to establish reasonable access requirements and manage risks of users to which TRs are exposed, in order to ensure their own financial soundness and conduct trade repository services in a stable manner.

## **(2) Major Supervisory Viewpoints**

- (i) When setting the access requirements, whether the TR examines whether the requirements are fair or not from the viewpoint of conducting trade repository services in an appropriate and reliable manner, etc., and releases the requirements to the public in consideration of such examination.
- (ii) Whether the TR abuses its position in such circumstances as using information received from trade repository services in other services and concluding contracts on services incidental to trade repository services.

## **(3) Supervisory Method and Actions**

In cases where a problem has been found in the user requirements, etc. the supervisory departments shall monitor voluntary business improvement made by the TR, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-80 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 156-81 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting public interest and investors.

## **VI-3-1-3 Prevention of Damage that May be Inflicted by Anti-Social Forces**

### **(1) Background and Objectives**

Eliminating anti-social forces from society is a task critical to ensuring the order and safety of society, so it is necessary and important to promote efforts to ban any relations with anti-social forces from the viewpoint of fulfilling social responsibility. In particular, as TRs are highly public in nature and play an important economic role, they need to exclude anti-social forces from financial instruments markets in order to prevent damage from being inflicted not only on themselves, their officers and employees but also on various stakeholders who participate in financial instruments markets.

Needless to say, if TRs are to retain public confidence and maintain the soundness and

appropriateness of their business operations, it is essential that they deal with anti-social forces in accordance with laws and regulations without bowing to pressure from them. Therefore, TRs must strive, on a daily basis, to develop a control environment for banning any relations with anti-social forces in accordance with the purpose of the “Guideline for How Companies Prevent Damage from Anti-Social Forces” (agreed upon at a meeting on June 19, 2007, of cabinet ministers responsible for anti-crime measures).

In particular, anti-social forces have become increasingly sophisticated in their efforts to obtain funds, disguising their dealings as legitimate economic transactions through the use of affiliated companies in order to develop business relations with ordinary companies. In some cases, the relations thus developed eventually lead to problems. In order to deal with such cases properly, the management teams of TRs need to take a resolute stance and implement specific countermeasures.

It should be noted that if a TR delays specific actions to resolve a problem involving anti-social forces on the grounds that unexpected situations, such as the safety of officers and employees being threatened, could otherwise arise, the delay could increase the extent of the damage that may be ultimately inflicted on the TR.

(Reference) “Guideline for How Companies Prevent Damage from Anti-Social Forces”  
(agreed upon at a meeting on June 19, 2007, of cabinet ministers responsible  
for anti-crime measures)

**(i) Basic Principles on Prevention of Damage that may be Inflicted by Anti-social Forces**

- Institutional response
- Cooperation with external expert organizations
- Ban on any relations, including transactions, with anti-social forces
- Legal responses, both civil and criminal, in the event of an emergency
- Prohibition of engagement in secret transactions with and provision of funds to anti-social forces

**(ii) Identification of Anti-social Forces**

In judging whether specific groups or individuals constitute “anti-social forces,” which are defined as groups or individuals that pursue economic profits through the use of violence, threats and fraud, it is necessary not only to pay attention to whether they fit the definition in terms of their affiliation, such as whether they constitute or belong to *boryokudan* crime syndicates, *boryokudan* affiliated companies, *sokaiya* racketeer groups, groups engaging in criminal activities under the pretext of conducting social campaigns or political activities, and crime groups specialized in intellectual crimes, but also to whether they fit the definition in terms

of the nature of their conduct, such as whether they are making unreasonable demands that go beyond the limits of legal liability. (Refer to the “Key Points of Measures against Organized Crime,” a directive issued in the name of the Deputy Commissioner-General of the National Police Agency on December 22, 2011.)

## **(2) Major Supervisory Viewpoints**

A TR should not have any relations with anti-social forces and, in cases where it has established a relationship with an anti-social force unwittingly, supervisors, while also giving consideration to the characteristics of specific transactions, shall pay attention to such as the following points in order to examine its control environment for banning any relations with anti-social forces as soon as possible after the counterparty has been found to be an anti-social force and its control environment for dealing with unreasonable demands by anti-social forces appropriately.

### **(i) Institutional response**

In light of the need and importance of an action to ban any relationship with anti-social forces organically, whether the responsibility of responding to the situation is not left solely to the relevant individuals or divisions but the management including directors are appropriately involved, and there is a policy for the entire organization to respond. In addition, whether there is a policy calling for the corporate group as a whole, not just the involved TR alone, to take on an effort to prevent any relationship with anti-social forces.

Furthermore, whether the TR is also making efforts to eliminate anti-social forces when conducting transactions including the provision of financial services under business alliance with other companies outside of the corporate group.

### **(ii) Developing of a Centralized Control Environment through anti-social forces response division**

Whether the TR has established a division in charge of supervising responses to ban any relationship with anti-social forces (hereinafter referred to as the “anti-social forces response division”) so as to develop a centralized control environment for preventing anti-social forces from inflicting damage, and whether this division is properly functioning.

In particular, whether the TR pays sufficient attention to the following points in developing the centralized control environment.

A. Whether the anti-social forces response division is actively collecting and analyzing information on anti-social forces and has developed a database to manage such information in a centralized manner and further, has a system to appropriately update it (i.e., addition, deletion or change of information in the database). Further, whether

the division is making efforts to share information within the group in the process of collecting and analyzing such information. Whether the anti-social forces response division has a system to appropriately take advantage of such information for screening the counterparties of transactions and evaluating the attributes of shareholders of the TR.

- B. Whether the TR makes sure to maintain the effectiveness of measures to ban any relations with anti-social forces by, for example, having the anti-social forces response division develop a manual for dealing with anti-social forces, provide on-going training, foster cooperative relationships with external expert organizations, such as the police, the National Center for the Elimination of Boryokudan, and lawyers, on an ongoing basis. In particular, whether the TR is prepared to report to the police immediately when it faces the imminent prospect of being threatened or becoming the target of an act of violence, by maintaining close communications with the police on a daily basis so as to develop a systematic reporting system and build a relationship that facilitates cooperation in the event of a problem.
- C. Whether the TR has a structure in which relevant information is appropriately conveyed to the anti-social forces response division for consultation when transactions with anti-social forces are found or such forces have made unreasonable demands. Further, whether the anti-social forces response division has a structure to appropriately report relevant information to the management. In addition, whether the anti-social forces response division has a structure to ensure the safety of individuals encountering anti-social forces in person and to support divisions involved in dealing with them.

**(iii) Execution of Appropriate Prior Screening**

Whether the TR bans allowing anti-social forces to become a participant or counterparty to a transaction by conducting appropriate advance screening using information on such forces in order to prevent transactions with anti-social forces, and makes sure provisions regarding the exclusion of “boryokudan” crime syndicates are introduced in all contracts and terms of transactions.

**(iv) Execution of Appropriate Follow-up Review**

Whether, for the purpose of making sure any relationships with anti-social forces are eliminated, there is a structure to conduct an appropriate follow-up review on existing claims and contracts.

**(v) Measures to Terminate Transactions with Anti-Social Forces**

- A. Whether the TR has a system under which information confirming the existence of a transaction with anti-social forces is appropriately reported to the management,

including directors, etc., via the anti-social forces response division, and responds to the situation under appropriate directions and involvement by the management.

- B. Whether the TR regularly communicates with external expert organizations, including the police, the National Center for the Elimination of Boryokudan, lawyers and so forth, and promotes efforts to eliminate any transactions with anti-social forces.
- C. Whether the TR, when it has learned through a follow-up review after initiating a transaction that the counterparty is a member of an anti-social force, takes measures to prevent the provision of benefits to anti-social forces, such as seeking collection to the extent possible.
- D. Whether the TR has a structure to prevent providing funds or engaging in inappropriate or unusual transactions for whatever reason if the counterparty has been found to be an anti-social force.

**(vi) Dealing with Unreasonable Demands by Anti-Social Forces**

- A. Whether the TR has a system under which the information that anti-social forces have made unreasonable demands is immediately reported to the management including directors, etc. via the anti-social forces response division and responds to the situation under appropriate directions and involvement by the management.
- B. Whether the TR actively consults external expert organizations, such as the police, the National Center for the Elimination of Boryokudan, and lawyers, when anti-social forces make unreasonable demands, and responds to such unreasonable demands based on guidelines set by the National Center for the Elimination of Boryokudan and other organizations. In particular, whether the TR has a structure to report to the police immediately when there is an imminent prospect of a threat being made or an act of violence being committed.
- C. Whether the TR, in response to unreasonable demands by anti-social forces, has a policy to take every possible civil legal action and to avoid hesitating to seek the initiation of a criminal legal action by proactively reporting damage to the authorities.
- D. Whether the TR ensures that the division in charge of handling problematic conduct promptly conducts a fact-finding investigation upon request from the anti-social forces response division, in cases where the unreasonable demand from anti-social forces is based on problematic conduct related to business activity or involving an officer or employee.

**(vii) Management of Shareholder Information**

Whether the TR manages shareholder information properly, through means such as periodically checking the transaction status of its own shares and examining information regarding the attributes of its shareholders.

### **(3) Supervisory Method and Actions**

When supervisory departments have recognized an issue of supervisory concern regarding a TR's control environment for banning any relations with anti-social forces, through inspection and daily supervisory administration, they shall identify and keep track of the status of voluntary improvement made by the TR by holding in-depth hearings and, when necessary, requiring the submission of reports based on Article 156-80 of the FIEA. When the TR is deemed to have a serious problem from the viewpoint of protecting the public interest and investors, because its internal control environment is extremely fragile, as shown by, for example, a failure to take appropriate steps toward dissolving relations with anti-social forces despite recognizing the provision of funds thereto and the presence of inappropriate business relations therewith, supervisory departments shall take actions, such as issuing an order for business improvement based on Article 156-81 of the FIEA.

## **VI-3-2 Business Continuity Management (BCM)**

### **(1) Background and Objectives**

TRs intensively accumulate and store over-the-counter derivatives transaction information and play a role in improving the transparency of the market based on said information. They are required to take such actions as formulating an appropriate business continuity plan (BCP) in order to recover their operations as soon as possible and continue their operations even in the event of an emergency, e.g., acts of terrorism and large-scale disasters.

### **(2) Major Supervisory Viewpoints**

- (i) Whether the TR recognizes what constitutes an emergency and is striving as much as possible to prevent or guard against any emergency by, for example, conducting inspections and anti-crisis practices periodically in normal times.
- (ii) Whether the TR formulates emergency response policies, etc., including a BCP, to recover their operations as soon as possible and continue their operations even in the event of an emergency, and periodically reviews them. In particular, whether the TR clarifies its decision-making system in crises.
- (iii) Whether the board of directors clearly defines the roles and responsibilities for addressing an emergency and endorses the TR's operational risk-management framework in the case of formulating and significantly changing the emergency response policies, etc.

- (iv) Whether the BCP, etc. aims to resume the operation of the indispensable information system within two hours from system halt.
- (v) Whether the TR has developed a control environment for promptly making a report to the Financial Markets Division of the Policy and Markets Bureau of the FSA and for making relevant organizations within the TR work closely with each other if an emergency has arisen or if the possibility of an emergency has been recognized.
- (vi) Whether the TR has established a backup center while taking geographic factors into account as a safety measure to prepare against emergencies. Whether the TR backs up business data in a timely manner and periodically conducts drills, such as switching over to the backup center.
- (vii) Whether the TR has considered measures assuming the possibility of electricity supply, communication lines, public transport and other social infrastructures coming to a halt.

### **(3) Supervisory Method and Actions**

When supervisory departments have recognized an issue of supervisory concern regarding a TR's control environment for crisis management, through daily supervisory administration, etc., they shall identify and keep track of the status of voluntary improvement made by the TR by holding in-depth hearings and, when necessary, requiring the submission of reports based on Article 156-80 of the FIEA.

When supervisory departments have recognized the occurrence of an emergency or the likelihood of an emergency occurring, they shall hold hearings periodically and check the situation first-hand so that they can identify and keep track of how the relevant TR is responding to the emergency, including whether the response (status of the development of a control environment for crisis management, securement of trade repositories operations, communications with relevant parties including users, dissemination of information, etc.) is sufficient in light of the level and type of the emergency, until the situation improves. In addition, they shall require the submission of a report based on Article 156-80 of the FIEA when necessary.

## **VI-3-3 Operational Risk Management**

### **(1) Background and Objectives**

Operational Risk is the risk of TRs, users, etc. incurring losses due to their officers and employees failing to conduct administrative work properly, causing accidents or committing illegal acts in the course of the administrative work process, and is deemed to be caused by various factors, such as information systems and internal procedures, in

addition to human errors.

It is important that TRs pursue sound and appropriate business operations by establishing arrangements and procedures for managing operational risks.

## **(2) Major Supervisory Viewpoints**

- (i) Whether the TR has established appropriate policies, procedures, etc. to identify and manage operational risks. Whether the TR examines them periodically, and reviews them as necessary. Whether the board of directors endorses such policies, procedures, etc., and clearly defines the roles and responsibilities for addressing operational risk. Also, whether the TR has implemented specific measures to reduce operational risks.
- (ii) Whether the TR has sufficient processing capacity to achieve a certain level of service in consideration of the volume of administrative processes, etc. expected in the future.
- (iii) In cases where the TR outsources part of its administrative processes to service providers or other third parties or relies on them, whether the TR confirms that the outsource fulfills the requirements that would have to be met if such processes were carried out by the TR itself.
- (iv) Whether the TR has specified a policy and procedures for selecting the business operations to be outsourced and the contractors to outsource them to, and concluded a contract and developed a control environment that enables sufficient management of such contractors.

## **(3) Supervisory Method and Actions**

In cases where a problem has been found in the response by the TR, the supervisory departments shall monitor voluntary business improvement made by the TR, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-80 of the FIEA.

Furthermore, the supervisory departments shall take actions, such as issuing an order for business improvement based on Article 156-81 of the FIEA, when the TR's control environment for managing operational risks is deemed to have a serious problem and the action is deemed to be necessary and appropriate from the viewpoint of protecting the public interest and investors.

## **VI-3-4 Information Technology Risk Management**

### **(1) Background and Objectives**

Information technology risk is the risk that TRs and users will incur losses generally



because of a computer system breakdown, malfunction or other inadequacies, or because of inappropriate or illegal use of computer systems.

TRs' systems are themselves market infrastructures that are indispensable for trade repositories operations, etc., so if any system troubles or cybersecurity incidents occur, they may inflict damage on TRs and users connected to the systems.

Therefore, it is important to build a robust control environment for managing information technology risks in TRs.

(Note) "Cybersecurity incidents" refers to instances of cybersecurity being threatened by so-called cyberattacks, including unauthorized intrusion, theft, modification and destruction of data, failure or malfunction of information systems, execution of illegal computer programs and DDoS attacks, committed via the Internet through malicious use of information communication networks and information systems.

## **(2) Major Supervisory Viewpoints**

### **(i) Recognition of Information Technology Risk**

- A. Whether the board of directors has formulated a basic policy for organization-wide management of information technology risk based on a full recognition of information technology risk.
- B. Whether the board of directors recognizes that prevention and efforts for speedy recovery from system troubles and cybersecurity incidents (hereinafter referred to as "system trouble, etc.") is an important issue and has developed an appropriate control environment.
- C. Whether there are arrangements and procedures for ensuring that information regarding information technology risk is properly reported to the management team.

### **(ii) Establishment of Appropriate Control Environment for Risk Management**

- A. Whether the TR has specified a basic policy for the management of information technology risk and developed a relevant control environment.
- B. Whether the TR has designated the types of risk that should be managed according to specific criteria and has identified the location of the risk.
- C. Whether the control environment for managing information technology risk is effective enough to, enable the TR to identify and analyze the actual state of its business operations and system troubles, and minimize the frequency and scale of system troubles in a manner suited to the system environment and other factors, thereby maintaining an appropriate level of computer system quality.

### **(iii) Assessment of information technology risk**

Whether the division managing information technology risk recognizes and assesses

risks periodically or in a timely manner by recognizing the fact that risks are becoming diversified due to changes in the external environment, such as seen in the examples of system troubles induced by large-scale transactions as a result of increased customer channels and efforts to enhance information networks that bring more diverse and broad-based impact.

Also, whether it is taking sufficient measures to address the risks that have been identified.

**(iv) Management of information security**

A. Whether the TR has developed a policy to appropriately manage information assets, prepared organizational readiness, introduced in-house rules, etc., and developed an internal control environment. Also, whether it is making continuous efforts to improve its information security control environment through the PDCA cycle, taking notice of illegal incidents or lapses at other companies.

B. Whether the TR is managing information security by designating individuals responsible for it and clarifying their roles/responsibilities in efforts to maintain the confidentiality, integrity and availability of information. Also, whether the individuals responsible for information security are tasked to handle the security of system, data and network management.

C. Whether the TR is taking measures to prevent unauthorized use of computer systems, unauthorized access, and intrusion by malicious computer programs such as computer viruses.

D. Whether the TR identifies important information of users it is responsible for protecting in a comprehensive manner, keeps its records and manages them.

Whether the TR, in identifying important information of users, has set business operations, systems and external contractors as the scope of protection and includes data, such as listed below, in the scope where it tries to identify those calling for protection.

- Data stored in the areas within the system that are not used in ordinary operations
- Data output from the system for analyzing system troubles, etc.

E. Whether the TR is assessing importance and risks regarding important customer information that has been identified.

Also, whether it has developed rules to manage information, such as those listed below, in accordance with the importance and risks of each piece.

- Rules to encrypt or mask information
- Rules for utilizing information
- Rules on handling data storage media, etc.

F. Whether the TR has introduced measures to discourage or prevent unauthorized access, unauthorized retrieval, data leakage, etc. such as listed below, for important information of users.

- Provision of access authorizations that limits access to the scope necessary for the person's responsibility

- Storage and monitoring of access logs

- Introduction of mutual checking functions such as by separating the individuals in charge of development and those responsible for operations, administrators and those responsible for operations, etc.

G. Whether TR has introduced rules for controlling confidential information, such as encryption and masking. Also, whether it has introduced rules regarding the management of encryption programs, encryption keys, and design specifications for encryption programs.

Note that "confidential information" refers to information, such as PIN, passwords, etc., whose misuse could lead to losses by users.

H. Whether the TR gives due consideration to the necessity of holding/disposing of, restricting access to, and taking outside, of confidential information, and treats such information in a stricter manner.

I. Whether the TR periodically monitors its information assets to see whether they are managed properly according to management rules, etc. and reviews the control environment on an ongoing basis.

J. Whether the TR conducts security education (including by external contractors) to all officers and employees in order to raise awareness of information security.

**(v) Management of cybersecurity**

A. Whether the board of directors, etc. recognizes the importance of cybersecurity amid increasingly sophisticated and cunning cyberattacks and has introduced the necessary control environment.

B. Whether the TR has introduced systems to maintain cybersecurity, such as listed below, in addition to making the organization more secure and introducing in-house rules, etc.

- Monitoring systems against cyberattacks

- Systems to report cyberattacks and public-relation systems when attacks occur

- Emergency measures by Computer Security Incident Response Teams and systems for early detection

- Systems of information collection and sharing through information-sharing organizations, etc.

C. Whether the TR has introduced a multi-layered defence system against cyberattacks that combines security measures respectively for inbound perimeter control, internal network security control and outbound perimeter control.

-Security measures for inbound perimeter control (e.g. introduction of a firewall, anti-virus software, Intrusion Detection System, Intrusion Protection System etc.)

-Security measures for internal network security control (e.g. proper management of privileged IDs/passwords, deletion of unnecessary IDs, monitoring of execution of certain commands, etc.)

-Security measures for outbound perimeter control (e.g. retrieval and analysis of communication/event logs, detecting/blocking inappropriate communication, etc.)

D. Whether measures such as listed below are implemented to prevent damage from expanding when cyberattacks occur.

-Identification of IP addresses from which the cyberattacks originate and blocking off of attacks

-Functions to automatically spread out accesses when under DDoS attacks

-Suspension of the entire system or its part, etc.

E. Whether necessary measures for vulnerabilities in the system, such as updating of the operating system and application of security patches, are introduced in a timely manner.

F. Whether the TR is, as part of cybersecurity measures, assessing its security levels by taking advantage of tests on network intrusion, vulnerability scanning or penetration tests, etc. and making efforts to improve security.

G. Whether the TR, when carrying out business operations using communication methods such as the Internet, has introduced appropriate authentication methods in line with the risks associated with such transactions, such as listed below.

-Authentication methods that do not rely on fixed IDs or passwords, such as variable passwords and digital certificates

-Transaction authentication using transaction signatures by means of a hardware token, etc.

H. Whether the TR, when carrying out business operations using communication methods such as the Internet, has introduced preventative measures in line with operations, such as listed below.

-Introduction of software that allows the TR to detect the state of virus infection of the user's PC and issue a warning

-Adoption of methods to store digital certificates in mediums or devices separate from the PCs used in the relevant business operation, such as IC cards

-Introduction of a system that allows the TR to detect unauthorized log-ins, abnormal input, etc. and immediately notify such abnormalities to users

I. Whether the TR has developed contingency plans against potential cyberattacks, conducts exercises and reviews such plans. Also, whether it participates in industry-wide exercises as necessary.

J. Whether the TR has formulated plans to train and expand the personnel responsible for cybersecurity and implements them.

**(vi) System Planning, Development and Operational Management**

A. Whether the TR has formulated a medium/long-term development plan after having clarified its strategic policy for systems as part of its management strategy. Whether the medium/long-term development plan has been approved by the board of directors.

B. Whether the TR reveals the risks inherent to its existing systems on an ongoing basis, and makes investments to maintain and improve the systems in a planned manner.

C. Whether the TR has clarified its rules for approval of plans, development and transition in development projects.

D. Whether the TR specifies the responsible person with respect to each development project and manages the progress based on the development plan.

E. Upon system development, whether the TR conducts tests in an appropriate and sufficient manner, such as by preparing test plans and making user divisions participate.

F. For human resources development, whether the TR formulates and implements specific plans to pass on the mechanism and development technologies of its existing systems and train personnel with expertise.

**(vii) Computer System Audits**

A. Whether an internal audit section that is independent from the computer system division and has auditing staff adept at computer systems conduct periodic audits of the computer system.

B. Whether the TR conducts internal audits by subject matter about computer systems and is taking of external audits by information system auditors.

C. Whether the audited division accounts for all business operations involving information technology risk.

**(viii) Management of Outsourcing of Business Operations**

A. Whether the TR selects outsourcees (including system subsidiaries) by evaluating and examining them based on selection criteria.

B. Whether the TR has prescribed the allocation of roles and responsibilities, audit authority, subcontracting procedures, level of services rendered, etc. with the

outsourcer in an outsourcing agreement. Also whether the TR presents to outsourced contractors rules and security requirements their employees are required to adhere to and security requirements, as well as defines them in contract forms, etc.

C. Whether the TR properly conducts risk management regarding outsourced business operations (including work further subcontracted) related to the computer system. In cases where system-related administrative processes are outsourced, whether the TR properly conducts risk management according to the outsourced business operations related to the computer system.

D. Whether the TR periodically monitors the outsourced business operations (including work further subcontracted) to determine, as the outsourcer, that the outsourced business operations are properly conducted.

Also, whether there is a system that allows the consigner to monitor and track the status of data of investors and users being processed at outsourced contractors.

**(ix) Contingency Plan**

A. Whether the TR has formulated a contingency plan and has established arrangements and procedures for dealing with emergencies.

B. Whether the TR is basing the details of its contingency plan on guides that allows it to judge objective levels of its details (such as "Guide to Formulate Contingency Plans at Financial Institutions" compiled by the Center for Financial Industry Information Systems).

C. Whether the TR, in developing a contingency plan, assumes not only contingencies due to natural disasters but also system troubles, etc. due to internal or external factors.

Also, whether it assumes risk scenarios of sufficient extent for cases such as a major delay in batch processing.

D. Whether the TR reviews assumed scenarios in its contingency plan by, for example, taking into consideration case studies of system troubles, etc. at other financial institutions, clearing organizations, fund clearing organizations, book-entry transfer institutions and trade repositories, and the results of deliberations at the Central Disaster Management Council, etc.

E. Whether exercises in accordance with the contingency plan involve the entire company and are periodically conducted jointly with outsourced contractors, etc.

F. Whether off-site backup systems, etc. are introduced for important systems whose failure could seriously affect business operations, and that a control environment is in place to address disasters, system troubles, etc. so that normal business operations can be speedily brought back.

**(x) Risk of System Updates, etc.**

- A. Whether the TR has developed a control environment for managing the risk of system updates, etc. by ensuring that its officers and employees fully recognize the risk.
- B. Whether the TR has established arrangements and procedures for conducting tests. Whether its test plan is suited to the nature of the system development necessitated by the system updates, etc.
- C. Whether the TR has established a control environment that enables itself to be proactively involved in the system updates, etc. when this task is outsourced.
- D. Whether the TR makes use of third-party evaluation, such as evaluation by a system auditor, when making judgment regarding important matters related to the system updates, etc.
- E. Whether the TR has developed a contingency plan for dealing with an unexpected incident.

**(xi) Response to System Troubles**

- A. Whether the TR implements appropriate measures to avoid creating unnecessary confusion among investors, users, etc. when system troubles, etc. occur and performs tasks towards the prompt recovery and operation of alternatives.  
Also, whether it has developed a worst-case scenario in preparation for system troubles and is prepared to take necessary measures accordingly.
- B. Whether the TR has prepared procedures that also subjects outsourced contractors to reporting system troubles, and has a clearly defined system of command and supervision.
- C. Whether the TR is prepared to immediately notify the representative director and other directors when a system trouble that may significantly affect business operations occurs, and report the largest potential risk it poses under the worst-case scenario (for example, if there is a possibility that the failure could gravely affect investors or users, etc., the reporting persons should not underestimate the risk but immediately report the biggest risk scenario).  
In addition, whether it is prepared to launch a task force, have the representative director issue appropriate instructions and orders, and seek resolution of the issue in a swift manner.
- D. Whether the TR, after system troubles, etc. have occurred, analyzes the cause and implements measures based on the analysis to prevent recurrence.  
Also, whether it periodically analyzes tendencies of factors that have led to system troubles, etc. and introduces measures to address them.
- C. Whether the TR immediately reports system troubles, etc. to the authorities.

### **(3) Supervisory Method and Actions**

#### **(i) At the Time of Problem Recognition**

When supervisory departments have recognized an issue of supervisory concern regarding a TR's control environment for managing information technology risk, through daily supervisory administration, etc., they shall identify and keep track of the status of voluntary improvement made by the TR, by holding in-depth hearings with the TR and the outsourcing contractor and, when necessary, requiring the submission of reports based on Article 156-80 of the FIEA.

When the TR is deemed to have a serious problem from the viewpoint of protecting the public interest and investors, the supervisory departments shall take actions, such as issuing an order for business improvement, etc., based on Article 156-81 of the FIEA.

#### **(ii) At the Time of System Updates, etc.**

In cases where TRs are to perform system updates, etc., they shall be required to submit specific plans for implementing the system updates, etc. and documents regarding the internal control environment for managing the risk associated with the system updates, etc. (including internal audits) and other matters according to their characteristics.

In cases where the system updates, etc. are large in scale, TRs shall be required to periodically submit reports based on Article 156-80 of the FIEA until such system updates, etc. are completed.

### **(4) Response to System Troubles**

- (i) TRs shall be required to notify the authorities of the occurrence of any computer system troubles as soon as they have recognized it, and submit a "Report on Problem Occurrence, etc." (in the format specified in Attached List of Formats 4-1) to the authorities.

After the computer system operation has been restored to normal and the cause of the problem has been identified, they shall be required to report to the authorities again. (It should be kept in mind that they shall be required to report to the authorities on the current state within one month even if the computer system operation has not been restored to normal or the cause of the problem has not been identified within the one-month period.)

(Note) Computer System Trouble Subject to Reporting to the Authorities

Problems that must be reported to the authorities are those which affect systems and equipment (including both hardware and software) used by TRs and contractors



undertaking business operations outsourced by TRs, and which could delay or suspend collection, storage, and reporting of transaction information and undermine the convenience of users, etc. in other ways.

However, the reporting requirement is not applicable to such system troubles in cases where a backup system has started up and effectively prevented adverse effects.

It should be noted that even if no computer system troubles have occurred, a report must be made in cases where users or business operations will be affected or are highly likely to be affected, including cases where a TR has received a warning of a cyber attack on its computer system or where it has detected the possibility of such an attack.

- (ii) A TR who has reported computer system troubles to the authorities shall be required to submit an additional report based on Article 156-80 of the FIEA when necessary. When the TR is deemed to have a serious problem from the viewpoint of protecting the public interest and customers, the authorities shall take actions, such as issuing an order for business improvement based on Article 156-81 of the FIEA.

When the TR is deemed to have committed a serious and malicious violation of law, the authorities shall consider necessary actions, including the issuance of an order for business suspension based on Article 156-83(1) of the FIEA.

### **VI-3-5 Appropriateness of Disclosure of Information, etc.**

#### **VI-3-5-1 Disclosure of Major Rules, etc.**

##### **(1) Background and Objectives**

It is important that TRs provide sufficient information so that users and prospective users can clearly recognize and fully understand the risks and responsibilities arising from their use of the trade repositories system.

Furthermore, from the viewpoint of providing sufficient information to users, etc., it is important that the rights and obligations of users, etc. and key procedures concerning risks, etc. are clarified and publicly disclosed in business rules and other rules and procedures.

##### **(2) Major Supervisory Viewpoints**

- (i) Whether the TR has formulated clear and comprehensive rules and procedures and disclosed them to users. Whether the TR publicly discloses key rules, procedures, etc.
- (ii) In the aforementioned rules, procedures, etc., whether the TR clearly describes the rights and obligations of the TR and users, so that users can assess the risks they would

incur by using the TR.

(iii) Whether the TR clarifies operations performed at a charge and operations performed without charge, and publicly discloses the fee and content of individual services.

(iv) Whether the TR periodically discloses information based on the “Principles for Financial Market Infrastructures” and the “Disclosure framework and Assessment methodology”<sup>(Note)</sup> that supplements the principles.

(Note) CPSS and IOSCO, “Disclosure framework and Assessment methodology” (December 2012)

### **(3) Supervisory Method and Actions**

In cases where a problem has been found in the disclosure of major rules, etc. by the TR, the supervisory departments shall monitor voluntary business improvement made by the TR, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-80 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 156-81 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting the public interest and investors.

## **VI-3-5-2 Disclosure of Market Data**

### **(1) Background and Objectives**

TRs should play an important role in improving the transparency of the market, and data accumulated by them should contribute to improving the transparency and stabilizing the financial system.

TRs are expected to accurately provide collected information to relevant authorities in a timely manner and make efforts to improve the transparency of the market for the general public as well.

### **(2) Major Supervisory Viewpoints**

(i) Whether the TR comprehensively and sufficiently provides collected information to relevant authorities from the viewpoint of improving the transparency of the market and stability of the financial system. Whether the TR takes due care to accurately disclose the collected information to an appropriate extent.

(ii) Whether the TR strives to develop a database suited to market players’ needs through communications with them from the viewpoint of disclosure of transaction information.

(iii) Whether the TR has a robust information technology system capable of accurately providing both past and up-to-date data. Whether the data can be provided in a timely manner in a form easy to be analyzed.

**(3) Supervisory Method and Actions**

In cases where a problem has been found with regard to the disclosure of market data by a TR, the supervisory departments shall monitor voluntary business improvement made by the TR, by holding an in-depth hearing regarding the cause of problems and improvement measures and, when necessary, requiring the submission of a report based on Article 156-80 of the FIEA.

Furthermore, the supervisory departments shall issue an order for business improvement under the provision of Article 156-81 of the FIEA when it is deemed necessary and appropriate to do so from the viewpoint of protecting the public interest and investors.

## **VI-4 Administrative Procedures**

### **VI-4-1 Points to Consider regarding Authorization of Business Rules, etc.**

#### **(1) Background and Objectives**

Business rules prescribe basic matters regarding the TR's trade repositories system, such as matters concerning contracts with financial instruments business operators which provide information, fees, and safety management of collected information, assuming authorization by the authorities.

In light of the above, TRs are required to clearly establish rules and procedures, etc. for business rules and clarify their basis and characteristics so that financial transactions can be conducted by users, etc. in a smooth, continuous and stable manner.

#### **(2) Major Supervisory Viewpoints**

- (i) When making amendment, etc. to business rules, whether the TR confirms that the trade repository system as a whole, including business rules and subordinate rules, etc. is consistent with laws and regulations, etc.
- (ii) Whether the TR discloses and as necessary explains such amendment, etc. to users, etc. in a clear and easy-to-understand manner at least after receiving authorization by the authorities, or as necessary before then
- (iii) When giving such explanation, whether the TR summarizes the basis and applicability of laws and regulations pertaining to contracts on trade repositories, etc.
- (iv) In cases where there is a foreign participant, whether the TR confirms the risks associated with differences in laws and regulations, including confirming the laws and regulations, etc. of the country concerned.
- (v) When confirming and explaining the above, whether the TR gives consideration to the accuracy of such confirmation and explanation by such means as utilizing outside experts as necessary.
- (vi) Whether the TR confirms that the provisions on the above are consistent with laws and regulations, etc. and as necessary explains them to users, etc.

## **VI-4-2 Points to Consider regarding Approval of Subsidiary Business**

### **(1) Purpose**

As TRs store and report transactional information, they play an important role in improving the transparency of the market, etc. Therefore, they are required to conduct business operations in a stable manner. As TRs handle business secrets of financial instruments business operators, etc. in the storage, etc. of transactional information, they are required to conduct business operations in an appropriate manner.

Considering their highly public nature as such, TRs must concentrate on trade repositories operations and business incidental thereto,<sup>(Note)</sup> and in principle, are not able to conduct any other business, for the purpose of blocking out risks from operations other than their core business (Article 156-72(1) of the FIEA).

On the other hand, based on the view that the provision of services other than their primary business may help improve the transparency of the market in light of users' needs, even if they do not correspond to trade repositories operations or business incidental thereto, TRs are able to conduct business that is found to have no risk of hindering their conducting of trade repositories operations in an appropriate and reliable manner, as related business, by obtaining approval.

(Note) What consists of business incidental to trade repository services needs to be examined with respect to each individual business, considering that the trade repository provides the services of collecting and storing transactional information.

### **(2) Application for Approval**

Upon making an application for approval, the TR shall submit the approval application form prescribed in Article 15(1) of the Cabinet Ordinance on Regulation on Over-the-Counter Derivatives Transactions (Attached List of Formats 4-2) and the attached documents listed in the items of Article 6(2) of said Order.

### **(3) Approval Screening**

Upon approval screening, it is necessary to determine the appropriateness of approval on a case-by-case basis, in view of such matters as whether there is a risk of hindering the TR from trade repositories operations in an appropriate and reliable manner. Specifically, approval screening shall be conducted from the following viewpoints.

- (i) Whether there is a high likelihood of causing losses for the TR and affecting its management.
- (ii) Whether the TR has identified the risks to which it will be exposed and established

arrangements and procedures for managing such risks properly.

- (iii) Whether there is a risk of undermining confidence in the fairness and impartiality of the trade repositories operations or undermining the social credibility as a TR because of the risk of the reliability and accuracy of transaction information being undermined.
- (iv) Whether the workload hinders the appropriate implementation of the trade repositories operations.
- (v) Whether the business, in light of its content and characteristics, helps the smooth implementation of the trade repositories operations. Whether the business helps facilitate the circulation of securities through increasing in the convenience for users.

With regard to the above screening, when the TR uses transaction information in subsidiary business, the supervisory departments shall pay attention to the following points from the viewpoint of whether the information is accurate and whether the information is abused, in light of the fact that TRs collect information based on their designation by the authorities in relation to the obligation for financial instruments business operators, etc. to report transactional information.

- (i) Whether the TR obtains consent from financial instruments business operators, etc. that access to the TR for using transactional information.
- (ii) When providing transaction information to a third-party entity, whether the TR obtains consent from financial instruments business operators that access the TR for doing so and accurately provides the information thereto. Whether the TR makes sure that the third party entity receiving the information takes measures to ensure safe management of transactional information.

#### **(4) Supervisory Method and Actions after Granting Approval**

TRs are important social infrastructures that improve the transparency of the market and ensure the stability of the financial system, and supervisory authorities are required to conduct monitoring on an ongoing basis so that the sound and appropriate operation of their primary business is not hindered due to other business operations, say, as a result of confidence in TRs being undermined.

In cases where other business conducted by a TR is hindering or has the risk of hindering the sound and appropriate operation of its primary business, the supervisory departments shall monitor voluntary business improvement made by the TR, by holding an in-depth hearing and, when necessary, requiring the submission of a report based on Article 156-80 of the FIEA.

Furthermore, the supervisory departments shall consider taking actions, such as issuing an order for business improvement under the provision of Article 156-81 of the FIEA,

when it is deemed necessary and appropriate to do so from the viewpoint of protecting the public interest and investors.