

Trading Participant Internal Management System Checkpoints

Japan Exchange Regulation

Trading Participants Examination & Inspection Department

Revised January 2026



Regarding the Revised Edition

The purpose of Japan Exchange Regulation (JPX-R)'s examinations and inspections is to ensure the fairness and reliability of the exchanges' markets by examining trading participants' compliance with laws and regulations as well as with the exchanges' rules (hereinafter "laws, rules, and regulations").

In particular, we believe that JPX-R's vital mission is to eliminate all inappropriate actions from the exchanges' markets and to require trading participants to enhance their internal management systems in order to prevent such actions from occurring. Furthermore, we also believe that it is important not only to point out violations of laws, rules, and regulations but also to support trading participants in developing the desired internal management systems.

Based on the knowledge that it had gained from past examinations and inspections, JPX-R's Trading Participants Examination & Inspection Department compiled the key points on internal management systems in matters related to compliance pertaining to exchange-based trading. They were published in 2009 as "Trading Participant Internal Management System Checkpoints" (hereinafter the "Checkpoints") and have been reviewed and revised as necessary. This latest edition has been revised in light of recent changes to the laws, rules, and regulations. In particular, the following sections have been revised: "5. Management of Best Execution Duties," 7.," and "12. Trading Supervision Systems."

We hope that the Checkpoints will serve as a useful reference for trading participants as they develop suitable internal management systems.

January 2026

Japan Exchange Regulation
Trading Participants Examination & Inspection Department

Contents

| | |
|---|----|
| 1. Short Sale Management | 4 |
| 2. Management of Corporate Information | 8 |
| 3. Management of Net Settlement Transactions | 12 |
| 4. Front Running Prevention | 15 |
| 5. Management of Best Execution Duties | 17 |
| 6. Management of Low Latency Trading | 21 |
| 7. IT Systems Risk Management System | 23 |
| 8. Management of Margin Transaction Security Deposit, etc. | 31 |
| 9. Error Correction Management (Correcting the Own-Account/Customer-Account Classification and Errors) | 34 |
| 10. Compliance with Same-Day Cash Collection Rules | 38 |
| 11. Measures to Prevent Erroneous Orders | 40 |
| 12. Trading Supervision Systems | 45 |
| 13. Management of Margins for Futures and Options Trading | 52 |
| 14. Credit Management for Margin Trading, etc. | 54 |
| 15. Internal Audit System | 57 |
| 16. Exchange System Connection Management | 60 |
| 17. Miscellaneous (1-2) | 63 |

★ Based on laws, rules, and regulations as of the end of December 2025.

Abbreviations

- TSE: Tokyo Stock Exchange
- OSE: Osaka Exchange
- JSCC: Japan Securities Clearing Corporation
- FSA: Financial Services Agency
- JSDA: Japan Securities Dealers Association
- FIEA: Financial Instruments and Exchange Act
- Order for Enforcement of the FIEA: Order for Enforcement of the Financial Instruments and Exchange Act
- FIB Cabinet Order: Cabinet Office Order on Financial Instruments Business, etc.
- Securities Transaction Restrictions Cabinet Order: Cabinet Office Order on Restrictions on Securities Transactions
- Security Deposit Cabinet Order: Cabinet Office Order on Security Deposits and Transactions Provided in Article 161-2 of the Financial Instruments and Exchange Act
- Supervision Guidelines: FSA's "Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc."

1. Short Sale Management

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 162.1.(1)
- Order for Enforcement of the FIEA: Article 26-2 through Article 26-6, others
- FIB Cabinet Order: Article 117.1.(24)-2 through (24)-5, Article 123.1.(26), others
- Securities Transaction Restrictions Cabinet Order: Article 9-2 through Article 15-8
- TSE Business Regulations: Rule 14.1.(2), and Rule 16
- TSE Rules Concerning Bids and Offers: Rule 8, others

(2) Regulatory Intent and Requirements

Short sales of securities are sales of securities that are not held and said to be effective in stabilizing price fluctuations in securities markets. On the other hand, there are also concerns that they can unduly exaggerate price declines and be used to intentionally collapse the price of an issue. Therefore, no person should carry out short sales that are in violation of provisions of laws and regulations. The sale of a security that has been borrowed or the sale of a security when it is not clear the security will be transferred immediately after selling holdings of the same security are also considered short sales.

Short sale regulations include not only an “obligation to specify and confirm” and “price limits” but also, established in 2008 in the wake of the global financial crises, prohibit naked short selling (short sales for which no arrangements have been made to secure the issues being sold) and require those holding short positions in excess of certain limits to provide balanced information to exchanges. Also included are short sales regulations at the time of capital increase through public offerings, which was established in 2011 in response to insider trading issues related to a capital increase through public offering (the prohibition of closing short positions, which are created by short sales conducted during the period from the announcement of a capital increase through public offering until the issuance price of the new securities is determined, using new shares among others obtained by subscribing to a capital increase through public offering).

“Obligation to specify and confirm” refers to a series of obligations that require trading participants to inform the exchange of whether or not a sale is a short sale and prior to this, to confirm with their customers before accepting orders whether sales will be short sales (the same applies to entrustment) and require customers (entrustors) to indicate whether or not sales are short.

“Price limits” refer to the prohibition of short sales below the most recently published price, excluding short sales at the most recently published price when that price is higher than the previously published price. In practice, this rule is applied under the “trigger-based” price regulation framework in which said limits are to be applied to an execution at a price at least 10% below the base price calculated using the preceding day's closing price of such stock.

It should be noted that there are provisions for transactions that are exceptions to the “obligation to specify and confirm” and to “price limits.” The requirements for these exceptions are provided to a limited extent in the Securities Transaction Restrictions Cabinet Order.

Regarding a stock that hits a trigger for a price limit, TSE will process an order as an error

if, upon acceptance of the order specifying that it is "subject to price regulation" (Flag: 5), a price limit for said limit order is triggered. In other words, specifying a short sale is effective and essential in order to comply with price limits.

In addition, the following points should be noted:

- i. Specification that a short sale is being undertaken must be made when the order is placed. For a sale that is being undertaken to correct a mistake in executing a customer order, and in essence will be a short sale on the trading participant's account, the trading participant must judge whether the sale is a short sale based on its amount outstanding for its own account at the time of execution. If a short sale is not specified as such beforehand, even if only in essence, the trading participant must immediately file a "Corrected Declaration for Short Sale/Margin Transaction Classification" to the exchange. When filing a correction, reporting a regulatory violation may be required.
- ii. When a trading participant undertakes a short sale on its own account to hedge ahead of time a purchase contract it will enter into for shares held by a customer, as part of a VWAP guarantee transaction or VWAP target transaction, the short sale is considered a sale order that is part of a predetermined program, and the order is managed in a special account. Furthermore, price regulations are not applied (but the short sale specification obligation does apply) to all day, morning session, and afternoon session VWAPs; however, hourly VWAP is subject to price limit regulations.
- iii. In cases of short selling for the purpose of hedging in advance of a transaction in which a proprietary purchase will be conducted outside the market at the closing price in the auction market (closing price guaranteed transaction), no exemption from price regulations will be granted.
- iv. As a general rule, short sale orders from an investor that is not a qualified institutional investor are exempt from the application of price limits as long as the size of each order is 50 or fewer trading units. However, if a customer has an order for more than 50 trading units and divides it into multiple orders for 50 or fewer trading units in order to evade regulations, such orders cannot be viewed as separate orders, and each order is not exempt from the application of price limits.
- v. Even if a price limit is not triggered yet when a trading participant is placing a short sale order, it is mandatory to clarify whether such short sale order is "subject to price regulation" (Flag: 5) or "not subject to price regulation" (Flag: 7), as prescribed in Rule 8 of TSE Rules Concerning Bids and Offers.
- vi. As one of the regulations for the prevention of naked short selling, when a trading participant receives an actual sale order involving securities for which a deposit request has not been received, the trading participant is required to confirm the method for managing the securities to be sold (the trust bank where the securities are being held) and whether the sale qualifies as an exception to the short sale specification and confirmation obligations. The trading participant must prepare and hold (for seven years) a record of its findings, in a manner that meets legal

requirements.

vii. When handling capital increase through a public offering, there is a need to inform customers of the regulations on short sales at each time of capital increase through a public offering. In addition, all trading participants must be vigilant toward whether or not there are acts to circumvent this regulation from trade surveillance perspectives. (While there are no obligations to proactively conduct checks, from the viewpoint of the soundness and propriety of operations, if a violation by a customer, which should have been easily detected in routine procedures, was undetected, there may be questions raised about inadequacies in the internal management system.)

(3) Key Management Checkpoints

- i. Are necessary organizational measures being in place to comply with short sale regulations?
- ii. Have appropriate internal rules on short sales been established? (internal regulations and operational rules on the types of short sales the firm handles; methods for confirming information, keeping records; and other relevant matters)
Has information on laws, rules, and regulations, notices from self-regulatory operations, etc. been organized and stored in a manner that is easy to find in administrative, sales, and other units in accordance with the firm's business activities?
- iii. Are prior short sale regulation violations used to identify problems, and have operations been revised in light of the frequencies and causes of these problems?
- iv. Does the firm conduct ongoing internal training on short sale regulations, and does it appropriately provide explanations and information to relevant units when there are revisions to laws and regulations?
- v. Have specific measures been taken appropriately in order to ensure that the firm's IT system prevents violations of short sale regulations, and has the verification of such measures been performed appropriately? For example, does the firm's IT system prevent the placement of a sell order whose size exceeds the amount of securities in trust, or does it automatically place a short sale flag on such sell orders?
- vi. In order to prevent naked short selling, how does the firm confirm the settlement arrangements for a short sale order before accepting it? How does it confirm whether the order is exempt from confirmation of settlement arrangements? In addition, are such confirmations recorded and retained appropriately?
- vii. How does the firm confirm the securities management method when brokering a long sale order whose size exceeds the amount of securities in trust and when brokering an order that is exempt from the application of short sale specification and confirmation obligations? In addition, is said confirmation recorded and retained appropriately?

- viii. Does the firm appropriately perform a check when an order is accepted and after the order is executed in order to determine whether a short sale by an investor that is not a qualified institutional investor has been divided into and placed as orders for 50 or fewer trading units, since such order placements are suspected of evading price regulations? When the firm discovers a transaction that looks suspicious, is an appropriate action taken, such as an examination of the transaction details?
- ix. When necessary, does the firm confirm whether an investor that makes a short sale is not a qualified institutional investor, such as by checking the information on qualified institutional investors on the FSA's website?
<http://www.fsa.go.jp/common/law/tekikaku/index.html> (only in Japanese)
- x. Is a check performed appropriately on a transaction that effectively became a short sale following an execution correction in order to prevent a failure to submit a report to the exchange regarding the correction?
- xi. When a customer has caused settlement failures (including in-store settlement failures) to occur on multiple occasions, does the firm manage them appropriately in terms of compliance with short selling regulations? For example, does the firm double check the appropriateness of the securities management method and of the contents of the settlement arrangements (Such double checking may include confirmation of such items as where to deposit the securities and where to obtain them, the agreement details, and operations.)? In addition, how does the firm handle such a customer?
- xii. Are customers handled appropriately and internal checks performed appropriately in terms of compliance with the obligation of holders of short positions at or above a certain threshold (0.2% or more and over 50 trading units) to provide the exchange with information on their balances?
- xiii. Are trading supervision and trade surveillance conducted appropriately in terms of preventing acts that hinder fair price formation, such as by checking whether there is any circumvention of short sale regulations?

2. Management of Corporate Information

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 38.1.(9) and Article 40.1.(2)
- FIB Cabinet Order: Article 1.4.(14), Article 117.1.(12) through (16), and Article 123.1.(5)
- TSE Trading Participant Regulations: Rule 22-5
- JSDA:
 - Rules Concerning Establishment of Confidential Corporate Information Management System by Association Members
 - Guideline for “Rules Concerning Establishment of Confidential Corporate Information Management System by Association Members”
 - Guidelines concerning Association Member Analysts’ Interviews, etc. with Issuers and Communication of Information
 - Rules Concerning Solicitation for Investments and Management of Customers, etc., by Association Members: Article 15, Article 15-2, and Article 25, others

(2) Regulatory Intent and Requirements

"Corporate information" means “undisclosed material information on the operation, business, or properties of listed companies, etc..., which is found to have an impact on customers' investment decisions; and undisclosed information about a decision on the implementation or suspension of a tender offer.” The scope of this definition is broader than the one that is used in insider trading regulations.

More specifically, under the provisions of FIB Cabinet Order Article 117.1.(12) through (16), which seek to prevent unfair trading and promote investor protection, corporate information cannot be used by executives and employees of financial instruments business operators for their personal trading, by financial instruments business operators for trading on their own accounts, or in brokerage operations.

FIB Cabinet Order Article 123.1.(5) requires that financial instruments business operators manage their operations in such a manner as to avoid the possibility that they may be cited for management of corporate information or management conditions of customers’ securities trading that lack measures necessary and appropriate for preventing unfair trading involving corporate information.

In addition, the following points should be noted:

- i. Each company is required to establish an appropriate management system for corporate information, including information that is not classified as corporate information at present but has a high possibility of becoming corporate information in the future, or for information (suggestive information) that is not corporate information in itself but can constitute a part of corporate information when combined with other corporate information obtained in advance.
- ii. Corporate information should be properly identified or recognized within companies

from substantial perspectives and should be put under proper management. Typically, corporate information, in addition to material facts that are subject to insider trading regulations, is thought to include information that could impact investment decisions (for example, matters that are not material facts pertaining to a listed company but would be included in an exchange's timely disclosures or ad hoc reports) and information on facts chronologically preceding the emergence of material facts (for example, in the case of a decision to be made by the executive organ of a listed company, information on facts indicating that the decision, which would amount to a material fact, is likely to be made in the near future).

- iii. "Unfair trading involving corporate information" includes insider trading. Therefore, if measures for preventing insider trading are found to be inadequate (for example, as evidenced by the failure to register insiders for multiple transactions), it is possible that FIB Cabinet Order Article 123.1.5 will also be found to have been violated.
- iv. Corporate insiders pertaining to J-REITs include related persons of a listed investment corporation (i.e., the J-REIT issuer), its asset management company, a parent company of such asset management company, and a specified related corporation (i.e., sponsor).
- v. Transactions based on discretionary trading agreements are transactions undertaken for customer accounts; but, if they are undertaken by a financial instruments business operator engaged in Type 1 financial instruments business, then they are included in the prohibitions on using corporate information for trading by a firm for its own account.
- vi. In the case of a financial instruments business operator engaged in Type 1 financial instruments business that is a listed company or the subsidiary of a listed company, the firm's own information may be considered corporate information and must be properly managed as necessary to prevent unfair trading in relation to such information.

(3) Key Management Checkpoints

- i. Have personnel been properly assigned and organizational measures taken to, for example: manage acquired corporate information; prevent unfair trading involving corporate information; accurately perform insider registration procedures; and supervise trading related to transactions by insiders?
- ii. Has the firm properly established internal rules (internal regulations or operating rules) to manage corporate information?
- iii. Are internal rules and points of attention regarding corporate information appropriately disseminated internally? Are operations conducted thoroughly in accordance with the internal rules on a companywide basis? (For example, even

outlets which normally handle small amounts of corporate information are required to establish systems so that corporate information is managed appropriately if and when it is acquired.

- iv. Are procedures for internally reporting when corporate information has been acquired by executives or employees in the course of their business activities being properly carried out? Also, in cases where management of such corporate information is conducted based on the ranking of its importance, is the ranking being conducted appropriately?
- v. Is communication prohibited both internally and externally, excluding cases where it is necessary for business operations and a predetermined procedure (such as obtaining approval from the administrative department) is followed? Also, is the easy communication of information from which corporate information can be inferred, or inquiries for corporate information or related information, prohibited?
- vi. Are documents and other media that contain corporate information and the related documentation for transactions in cases where the firm is involved in an important transaction by an issuer (merger, acquisition, tender offer, new share or other issuance, management change, or important matter involving the issuer) being appropriately managed (for example, whether individual organizational units manage documentation by physically isolating it from other organizational units) by considering its own internal organization and the frequency of obtaining corporate-related information (e.g., by considering the location, layout, access restrictions (e.g., under lock and key), and document management)?
- vii. Are electronic files that include corporate information properly managed to prevent their being seen by units, departments, or divisions that do not need them for business operations, through access restrictions, for example? Also, in cases of granting IDs with special privileges, such as access to all servers and folders for the purpose of system maintenance, is management appropriately conducted to prevent information leaks, such as password setting or access log monitoring?
- viii. When investment material is to be prepared and distributed internally, is such information inspected (including whether there is leakage or communication of corporate information through the investment material) by a controlling unit, department, or division responsible for managing corporate information? In addition, is internal information disclosure performed all at the same time?
- ix. Is there a proper structure to check if information an analyst obtained through a meeting with an issuer includes corporate information?
- x. Are proper checks conducted in a timely manner when an analyst provides information to customers through means other than an analyst report (for example, via phone or e-mail)?
- xi. Is trading supervision (addressing, for example: 1. trading on the firm's own account; 2. use of corporate information for brokerage operations; 3. trading by

the firm's executives and employees; and, 4. measures for preventing the communication of corporate information to other parties) to prevent unfair trading involving corporate information being properly performed in accordance with internal rules?

- xii. In the event of a release based on published information, are proper checks made by means such as TSE's disclosure information browsing service (TDnet)?
- xiii. Is work related to the registration of insiders being properly performed in accordance with internal rules? In addition, are regular inspections of the registration details for insiders (including reconciliation with J-IRISS) being properly performed? (Note: On May 25, 2026, the reconciliation method is scheduled to change from reconciliation with J-IRISS to reconciliation with the Executive Information Database.)
- xiv. Is there a requirement that customers must immediately notify the trading participant when there are changes regarding whether or not they must be registered as insiders? How is the fulfillment of the relevant obligations ensured? (Is this issue addressed in written agreements, through the use of confirmations, or from website entries? How is this issue handled in the case of internet-based trading, in particular?) In addition, how are cases in which notification to a customer was overlooked handled?
- xv. How are transactions by customers registered as insiders handled?
- xvi. How are cases in which there was a failure to secure a copy of the Customer Order handled?
Also, how does the firm handle ex-post investigations involving issues for which corporate information has been publicly released?
- xvii. Does the firm properly monitor for, and perform investigations to determine whether it has accepted, trading orders in which it is clear that an executive or employee of an issuer can profit from a trading order that involves the issuer's specified securities and is either a sell order falling within six months of a buy order or a buy order falling within six months of a sell order?
- xviii. Is monitoring, such as regular inspections, conducted to determine whether management irregularities are occurring in relation to the management of corporate information or if appropriate management is being conducted?

3. Management of Net Settlement Transactions

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 161-2
- Security Deposit Cabinet Order: Article 10.1.

(2) Regulatory Intent and Requirements

"Net settlement transactions", which, under the law, are transactions not specified as margin transactions, are prohibited. If a financial instruments business operator undertakes a cash transaction to buy or sell securities based on a customer order, and then undertakes a closing transaction for the same issue, settlement cannot be made by omitting actual delivery of the securities and simply offsetting the transactions.

In other words, orders that are not specified as margin transactions when made should be settled through the actual exchange of funds and securities. Unwholesome transactions that include no delivery of securities and no margin trading deposits, despite being essentially margin transactions, are prohibited.

Net settlement transactions may undermine wholesome investment behavior by skirting margin trading deposit regulations and promoting speculative trading and, therefore, are illegal.

In addition, the following points should be noted:

- i. If purchase funds are required to be deposited in a money reserved fund (MRF) or other such account, deposits of the necessary amounts must be made into these cash accounts by settlement time.
- ii. Whether multiple trades of the same issue on the same day (intraday trading) amount to net settlement transactions must be determined during that day. For example, if intraday trading involves a sale of 1,000 shares, a purchase of 1,000 shares, and another sale of 1,000 shares, a total of 2,000 shares are being sold while 1,000 shares are being purchased, and net settlement transactions will not have taken place if the sales of 2,000 shares are settled with 2,000 shares that were already on hand. However, if only 1,000 shares were on hand, net settlement transactions will have occurred. Similarly, in the case of a purchase of 1,000 shares, a sale of 1,000 shares, and another purchase of 1,000 shares, if purchase funds of only 1,000 shares are settled, net settlement transactions will have occurred.
- iii. For cases in which a customer sells shares already on hand, and then repurchases them on the same day (including cross trades), the movement of shares on hand must be properly recorded in the account transfer ledger and other accounting documentation when there is no deposit of funds for the purchase.
- iv. If a customer fails to make settlement (an advance is recorded) and a sale to effect a closing transaction was properly executed on the customer's account pursuant to

Rule 53 of the TSE Brokerage Agreement Standards, then no net settlement transactions will have taken place.

v. In exchange trading, netting settlements between customers who are participants of Japan Securities Depository Center's "DVP settlement scheme for NETDs (non-exchange transaction deliveries)" based on said scheme, are not viewed as illegal. (Response from JSDA Business Rules Referral System dated September 12, 2003)

(3) Key Management Checkpoints

- i. Have appropriate organizational measures been taken to prevent net settlement transactions?
- ii. Have internal rules been properly established (internal regulations or operating rules) to prevent net settlement transactions?
- iii. How is intraday trading handled? In particular, if a firm-specific management approach is used, is it appropriate?
- iv. Are advances to customers (including situations in which advances may be made) and sales to effect closing transactions properly handled in accordance with TSE Brokerage Agreement Standards?
- v. Are fund deposits and payments properly handled and managed to avoid net settlement transactions?
- vi. How are searches for transactions that are possibly net settlement transactions (checks to determine whether required funds have been deposited before settlement) performed?
- vii. Are 1) margin transactions in which shares are actually received and sold, 2) cash purchases and actual deliveries, and 3) the actual receipt and actual delivery of the same shares, all of which resemble net settlements, appropriately performed and managed?
- viii. When a net settlement transaction occurs, is it properly handled within the firm?
- ix. Are appropriate internal communications (among different units) and other internal systems and measures in place to handle cases in which it is difficult to judge whether net settlement transactions have occurred?
- x. Is internal training conducted, are specific cautions issued for individual cases, and are other steps being properly taken to prevent net settlement transactions?
- xi. How are cautions issued to customers (for example, via a website) to prevent net settlement transactions?

xii. When internal inspections are conducted regarding net settlement transactions, what do they focus on and with what frequency are they being performed?

4. Front Running Prevention

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 38.1.(9)
- FIB Cabinet Order: Article 117.1.(10)
- Supervision Guidelines: IV-3-1-3 Discretionary Trading Contracts (1)

(2) Regulatory Intent and Requirements

To prevent conflicts of interest between financial instruments business operators pursuing brokerage and trading operations and their customers, the FIB Cabinet Order prohibits financial instruments business operators from placing trades for their own accounts ahead of trading for customer orders. This order was put in place to protect customers from higher execution costs that would result if a financial instruments business operator, after receiving a customer's order, abuses the order information and places an order for the same sale or purchase for its own account ahead of the customer's order, but at similar or more advantageous terms.

It should be noted that trading orders based on the discretionary trading agreements (all discretionary trading agreements with related foreign financial instruments business operators) addressed in Article 16.1.(8).b of the Cabinet Office Order regarding Definitions Provided in Article 2 of FIEA are regarded as equivalent to orders for a financial instruments business operator's own account and are subject to front running regulations.

In addition, the following points should be noted:

- i. Regulations cover not only securities purchases and sales but also market derivatives transactions and foreign market derivatives transactions.
- ii. Prevention of front running requires the establishment of separate units for handling customer orders and handling orders for a firm's own account, as well as proper management of customer order information. At a minimum, this requires the separation of operations for handling the two types of orders and an information firewall (physical and system-based).
- iii. If a financial instruments business operator that has received a stop order uses information related to that order to trade for its own account before or after the trigger price (the market price specified by a customer as the "trigger" for immediate execution of the customer's buy or sell instructions) is reached, and before executing the customer's stop order, it may be found to have engaged in front running.
- iv. If an accommodative transaction undertaken to accommodate a trade with single price execution (Note A) is executed ahead of the entrusted CD order (Note B) or VWAP order for the same issue and in the same direction, the accommodative transaction for the firm's own account and the entrusted CD order or VWAP order must not be handled by the same person.

(Note A) This refers to a customer's request for an off-auction transaction or off-exchange transaction after a trading session at the average price for an accommodative transaction completed by the financial instruments business operator. The financial instruments business operator must undertake an accommodative transaction for its own account on the exchange.

(Note B) This refers to an order that a financial instruments business operator has been requested to handle with best execution, and its own discretion on pricing, within a day's trading.

Reference: TSE and OSE have separate rules (TSE/OSE Rules Concerning Just and Equitable Principles of Trade) addressing front running involving price-linked products (for example, derivatives and listed stocks) in two markets.

(3) Key Management Checkpoints

- i. Whether the information firewall measures¹ in the form of physical locations of units for handling customer orders and handling orders for the firm's own account² and the seating locations of employees are adequate for compliance with front running regulations.
- ii. When a failure occurs in the system that handles customer orders, does a unit in the division that handles orders for the firm's own account also handle customer orders as an emergency measure? If so, what rules govern the handling of such customer orders in relation to orders for the firm's own account?
- iii. Have internal rules (rules on the management of order information to prevent leaks and abuse of order information, and penalties for violation) and procedure manuals been properly prepared for the prevention of front running?
- iv. Is there prompt action to ensure that employees thoroughly understand revisions of relevant rules?
- v. Are internal checks to identify possible front running activity performed, and how are discovered cases addressed?

¹ Separation and independence of offices or floors, assignments of dedicated supervisors and employees, and controls preventing unauthorized employees from entering offices or floors

² Examples of units handling trades for a firm's own account include: 1) dealing units; 2) units that execute trades based on discretionary trading agreements with related foreign financial instruments business operators; 3) units that handle prior accommodative transactions for the firm's own account in connection with orders for which the firm is on the other end of a transaction for which the ToSTNeT (off-auction trading) price is predetermined; 4) units that handle prior accommodative transactions for the firm's own account in connection with orders for trades with single price execution; and 5) units handling trades for the firm's own account in connection with execution corrections (trades that rectify an incorrectly executed customer order by transferring the error to the firm's own account).

5. Management of Best Execution Duties

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 40-2
- Order for Enforcement of the FIEA: Article 16-6
- FIB Cabinet Order: Article 70-2 and Article 124
- Supervision Guidelines: IV-3-1-2 Control Environment for Customer Solicitation and Explanations

Reference: Financial System Council's Working Group on Capital Market Regulations "Report of the Task Force to Discuss Optimal Ways to Ensure Best Execution," dated June 2, 2021 (only in Japanese)

(2) Regulatory Intent and Requirements

"Best execution duties" refer to the duties of financial instruments business operators to take reasonable care to execute their customers' securities transactions on the best possible terms.

Since financial instruments business operators act as mandataries of securities transactions, they have a duty to their customers to take "the due care of a prudent manager" as stipulated in Article 644 of the Civil Code, which states that "a mandatary bears a duty to administer the mandated business with the due care of a prudent manager in compliance with the main purport of the mandate." Best execution duties are regarded as part of the prudent manager's duties that are borne by financial instruments business operators.

The FIEA stipulates the five specific duties of financial instruments business operators, which are: (1) to establish a policy and a method for executing orders under the best terms and conditions (hereinafter "best execution policy"); (2) to disclose their best execution policy; (3) to provide a customer with information on their best execution policy before accepting the customer's order; (4) to execute orders in accordance with their best execution policy; and (5) to provide an explanation stating that an order was executed in accordance with their best execution policy and other information pertaining to matters specified by Cabinet Office Order, if a customer requests such information after the order was executed.

Based on the recommendations of the Financial System Council's Working Group on Capital Market Regulations "Report of the Task Force to Discuss Optimal Ways to Ensure Best Execution," which was published in June 2021, the Order for Enforcement of the FIEA, the FIB Cabinet Order, and the Supervision Guidelines were issued in May 2022, and revisions pertaining to best execution policies came into effect in January 2023. The revisions clarified the matters to be included in best execution policies when using a smart order routing (SOR) system and when executing orders from retail customers.

(3) Key Management Checkpoints

- i. Formulation of the Best Execution Policy:
- a) Which department performs the final check to assess the appropriateness of the written contents of the best execution policy? In addition, have the rules and notices related to best execution duties been circulated and retained appropriately within the relevant departments?

 - b) Has the firm's best execution policy been revised in light of "Points of Attention Regarding the Best Execution Policy, etc." (January 2023 revision of Supervision Guidelines IV-3-1-2 (11))?
- ii. Publicization of the Best Execution Policy:
- a) Has the best execution policy been publicized appropriately using all of the following methods?
 - Posting or making it available for inspection at an easily visible location at the firm's head and branch offices
 - Posting or making it available for inspection at an easily visible location at the firm's sales offices
 - Publishing it on the firm's website
- iii. Provision of the Best Execution Policy:
- a) Does the firm provide customers with information on its best execution policy appropriately? (The firm must also provide customers with information on any updates to its policy.)

 - b) Is management performed appropriately in order to prevent the firm from accepting an order from a customer who has not been provided with information on the firm's best execution policy, either because the firm failed to provide the customer with the information or because the provided documentation was returned due to a change in address or other reason?
- iv. Execution of Orders in Accordance with the Best Execution Policy:
- a) In what way has the internal management system been developed so that orders are executed (and checked) in accordance with the best execution policy?

 - b) When a new stock is to be listed simultaneously on multiple exchanges, how is the market determined in which orders will be executed?

 - c) When an order is executed in accordance with the customer's instructions, it is recorded and managed appropriately?

 - d) When a customer's order cannot be executed in accordance with the best execution policy during a system failure, how is it managed? In addition, how is the customer's original order processed?
- v. Explanation Stating That an Order Was Executed in Accordance with the Best Execution Policy (Provided to Customers):
- a) When a customer requests an explanation stating that the customer's order

was executed in accordance with the firm's best execution policy, has a management system been established to enable the firm to respond appropriately? In light of the January 2023 revision of the FIB Cabinet Order, when the firm uses SOR, does the explanation that it provides to customers include both the execution price and the best price at each financial instruments exchange market that it had checked?

Reference: System Development That Is Required of Trading Participants That Conduct Dark Pool Transactions

| Item | Details |
|---|--|
| Flagging a dark pool transaction | When a trading participant submits a bid or offer to execute a single stock transaction or basket transaction in the ToSTNeT market or to execute a transaction in the J-NET market, the trading participant must clearly indicate to the Exchange whether the bid or offer is made via a dark pool (by flagging it). |
| Explaining the conditions for forwarding an order to a dark pool and providing operational information on the dark pool | A financial instrument business operator or other entity that forwards a customer's order to a dark pool (hereinafter the "dark pool forwarder") will be required do the following: <ul style="list-style-type: none"> - Understand the operational status of the dark pool to which the order is forwarded - Provide an appropriate explanation regarding the conditions for forwarding an order to a dark pool and provide operational information on the dark pool (e.g., information on the dark pool operator and on its participants) based on such factors as the customer's knowledge and experience |
| Recording and retaining information in order to ensure the effectiveness of price improvements | In order to enable a requesting customer or the authorities to confirm the status of price improvements after an order's execution, the dark pool forwarder is required to do the following; unless the customer prioritizes another matter over price improvements. <ul style="list-style-type: none"> - Record and retain the price and time of the order when it was matched in the dark pool - Record and retain the prices and times of the order at financial instruments exchanges, proprietary trading systems (PTSs), and dark pools when the decision was made to forward the order to a dark pool |
| Explaining to customers about the effects of price improvements | A customer who made dark pool transactions primarily for the purpose of price improvements will be provided with a clear explanation about the effects of price improvements on each transaction. |

6. Management of Low Latency Trading

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 2.41 through 42, Article 38.1.(8), Article 40.1.(2)
- FIB Cabinet Order: Article 116-4, Article 123.1.(14), Article 158.4, Article 338.6 through 7
- Supervision Guidelines: IV-3-2 Appropriate Exercise of Market Intermediary Function of Securities Companies, etc.
- FSA Guidelines for Supervision of High Speed Traders
- TSE Business Regulations: Rule 14.1.(7)
- OSE Business Regulations: Rule 26.1.(2)
- TSE Trading Participant Regulations: Rule 21-2
- OSE Trading Participant Regulations: Rule 19-2

(2) Regulatory Intent and Requirements

The impact of low latency trading of stocks, etc. has become more significant in recent years amid the advances in trading systems. However, there was no framework for regulatory authorities or exchanges to directly collect information from low latency traders, rendering a situation where it was not possible to ascertain the actual state of low latency trading. The issue was discussed by the Working Group on Financial Markets under the Financial Systems Council. The results of the discussion were summarized in a report, which pointed to a need for regulatory measures and led to the partial revision of FIEA.

Thereafter, in April 2018, a registration regime for low latency traders was introduced, which requires entities who fit the definition of persons conducting low latency trading stipulated in laws and regulation to register as such with the regulatory authorities.

In addition, the following points should be noted:

- i. Accepting orders for low latency trading from non-registered firms or from registered firms who have been issued a business suspension order or whose systems have yet to be verified is prohibited. When accepting orders from persons conducting low latency trading, a timestamp (the time at which an order is accepted by a financial instruments exchange, etc.) must be included in the statutory books or records (i.e., order forms) with the same number of digits as those notified by the financial instruments exchange, etc.
- ii. When a trading participant accepts an order of low latency trading from a low latency trader, it must indicate if the trading strategy for such order falls under: Market Making, Arbitrage, Directional, or Other.
- iii. Trading participants must take appropriate action such that persons conducting low latency trading can respond to requirements made by the exchange, etc.

(3) Key Management Checkpoints

- i. When starting to accept, etc. orders for low latency trading from persons who will conduct trading that constitutes low latency trading, does the trading participant confirm whether said persons are not entities other than persons conducting low latency trading as stipulated in FIEA Article 38.(8) or those defined as persons conducting low latency trading in FIB Cabinet Order, Article 116-4 (1) and (2) (hereinafter "non-registered traders, etc.")? The following are examples of the situation prescribed in Article 116-4 (2) where it is not possible to verify whether appropriate measures are being implemented to sufficiently manage electronic information processing systems and other systems for low latency trading:
 - a) Where it is not possible to verify in writing, etc. whether said person takes measures to sufficiently manage the trading system it specified at the start of trading as a system for managing low latency trading
 - b) Where it is not possible to obtain an appropriate report or explanation in writing, etc. when said person's trading system malfunctions after the start of trading

- ii. If after having accepted, etc. orders for low latency trading from persons conducting low latency trading said persons are found to meet the criteria for unregistered traders, etc., does the trading participant take measures to immediately suspend accepting, etc. orders from said persons (by, for instance, including a clause in the contract or other documents with persons conducting low latency trading that requires a person conducting low latency trading who has met the criteria for unregistered traders, etc. to agree to immediately inform the securities company, etc. of such matter)?

7. IT Systems Risk Management System

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 40.1.(2)
- FIB Cabinet Order: Article 123.1.(14)
- Supervision Guidelines: III-2-8-1 Control Environment for Managing Information Technology Risk, III-2-8-2 Internet Transactions, others
- FSA: "The Policy Approaches to Strengthen Cyber Security in the Financial Sector" (English summary available)
- FSA: "Guidelines on Cybersecurity for the Financial Sector"
- JSDA: Guidelines to Prevent Unauthorized Access and Other Incidents in Online Trading

(2) Regulatory Intent and Requirements

The order receipt and execution services that financial instruments business operators offer to customers are the most basic, yet important services, and in recent years the dependence on systems in the financial instruments business has been increasing. Under these circumstances, financial instruments business operators are required to establish risk management systems to prevent system malfunctions or other erroneous operations.

Additionally, with the recent increase of algorithmic and high-frequency trading, the risks involved with system errors has increased. Trading participants are requested to appropriately conduct management so as not to obstruct exchange trading systems or price formation, to ensure stable market operations. Furthermore, there have been incidents of large-scale cyber-attacks and unauthorized access, and in some cases, the incidents were exploited for unfair trading. In terms of the financial system's reliability, such incidents cannot be disregarded. As a result, it has become extremely important to ensure cyber security.

In addition, the following points should be noted:

- i. Conditions under which management of electronic data processing systems is deemed to be inadequate under the relevant laws and regulations include, for example, situations in which appropriate electronic data processing systems have not been established in light of the points enumerated in the Supervision Guidelines (Supervision Guidelines: IV-3-2-1-(3))
- ii. In cases where internet trading services are being provided, it is also necessary to consider the JSDA's "Guidelines to Prevent Unauthorized Access and Other Incidents in Online Trading".
- iii. Regarding the management of cyber security, it is also necessary to consider such FSA publications as "The Policy Approaches to Strengthen Cyber Security in the Financial Sector" and "Guidelines on Cybersecurity for the Financial Sector."
- iv. When a system malfunction occurs, it is necessary to submit a "Malfunction Report" to government authorities. In doing so, it is also necessary to submit a "Computer

System Malfunction Report" to the exchange (TSE).

(3) Key Management Checkpoints

*For details, refer to Supervision Guidelines, III-2-8 Control Environment for Managing Information Technology Risk, (1) Major Supervisory Viewpoints.

i. Sufficient Recognition of IT Systems Risk

- a) Is the board of directors sufficiently aware of IT systems risk, and has it formulated a basic policy for company-wide risk management? In addition, does the board of directors recognize that system failures and cyber security incidents³ are significant management issues, and has it established a system to prevent them and to quickly recover from them if they occur?⁴ Furthermore, has the board of directors appointed an executive who is sufficiently aware of the importance of systems risk, has sufficient knowledge of and experience with computer systems, and can execute his or her duties appropriately as the executive in charge of supervising and managing the firm's computer systems? Has the board of directors also specified in detail the responsibilities to be fulfilled and the measures to be taken when a system failure or other crisis occurs? Has it ensured the effectiveness of said measures by conducting drills as needed in which it assumes command itself?

ii. Establishment of Risk Management System

- a) Is the basic policy for IT systems risk management defined and has a management system been established? Does the basic policy for IT systems risk management include a security policy (a basic policy to properly protect information assets in the organization) and a policy regarding outsourcees?
- b) Has a IT systems risk management framework been developed based on contents that can be judged objectively? Also, is this framework consistently reviewed in response to the identification and analysis of system malfunctions, implementation of risk management, and improved technology, among other things?

iii. IT Systems Risk Assessment

- a) Does the IT systems risk management division understand and assess risk in a regular or timely manner as risks diversify with changes in the external environment (including large amounts of transactions arising from diversification of customer channels, and broader and more complicated impact

³ A cyber security incident refers to an incident in which cyber security is threatened by a cyber-attack conducted via cyberspace through the misuse of telecommunications networks and information systems. Examples of cyber-attacks include unauthorized access; the theft, falsification, or destruction of data; causing information systems to stop operating or malfunction; the execution of malicious programs; and DDoS attacks.

⁴ Analyses of recent incidents of unauthorized access by malicious third parties have stated that they were caused not only by a lack of technical measures to prevent the unauthorized access but also by the insufficient involvement of the firm's management.

of system malfunctions due to network expansion)? In addition, are there sufficient measures for recognized risk?⁵

iv. Information Security Management

- a) For appropriate management of information assets, are there policies, organizational structures, internal rules, and internal management systems? In addition, are the information security management systems improved regularly through PDCA cycles with reference to improprieties or incidents at other companies?
- b) Is internal information managed by assigning persons in charge of managing information security and clarifying roles and responsibilities to maintain confidentiality, integrity, and availability of information? In addition, do said persons conduct overall supervision of systems, data, and network security?
- c) Are there any measures to prevent unauthorized use of computer systems, unauthorized access, and intrusion by malicious software (including computer viruses)?
- d) Does the financial instruments business operator comprehensively identify, grasp, and manage important customer information, for which the financial instruments business operator is responsible? In addition, does the financial instruments business operator conduct prioritization and risk assessment of important customer information that has been identified? Moreover, is there a structure to check, prevent, and control unauthorized access, unauthorized obtainment, and information leakage regarding important customer information?
- e) Are there management rules for confidential information (encryption or masking)? In addition, are there management rules for encryption programs,

⁵ When IT systems risk is assessed, the following four points should be noted:

1) Completeness of assessment

All systems including those that are outsourced need to be comprehensively checked, and systems that handle important information in terms of cyber security and will have a critical influence in the case of a system failure need to be included in the risk assessment as appropriate.

2) Implementation of assessment

These systems shall be appropriately assessed by analyzing (rating, etc.) the criticality, vulnerability, and threat status, among other aspects. In addition, risk countermeasure standards such as information system management standards shall be established, and risk mitigation measures shall be implemented and confirmed. Assessment after risk mitigation shall be conducted (identifying residual risks) to clarify whether or not further countermeasures are necessary.

3) Formulation and implementation of response plan

Based on the assessment results, a response plan for IT systems risks shall be formulated, and measures shall be implemented based on said response plan.

4) Reporting to management

The results of the assessment and the progress of the response plan shall be reported to management appropriately.

encryption keys, and design documents for encryption or other security programs? Moreover, is there tighter management on storage and disposal, access restrictions, and bringing confidential information outside the company that sufficiently considers operational necessity?

- f) Are information assets monitored regularly with regard to whether they are appropriately managed based on management rules, and is the management system reviewed continuously? In addition, are education programs on information security held for all employees (including education for outsourcees) to raise awareness about security?

Reference: "FISC Security Guidelines on Computer Systems for Financial Institutions" (published by The Center for Financial Industry Information Systems)

v. Cyber Security Management

- a) Does the board of directors recognize the importance of cyber security, and has it established the necessary system based on the "Guidelines on Cybersecurity for the Financial Sector?"⁶
- b) When the firm conducts a non-in-person transaction using the Internet (hereinafter "internet transaction"), has it established a system for ensuring that it is handled appropriately in accordance with the provisions of Supervision Guidelines III-2-8-2-2?

Note: The Japanese HTML and PDF versions of the Supervision Guidelines have been updated to include Section III-2-8-2-2 and are available on the FSA's website. However, the official English PDF version had not yet been updated as of the date of this document. In the meantime, please refer to the Japanese version until the official English version becomes available. Please also note that the FSA's website offers machine translations of its Japanese webpages by clicking on the Language icon and choosing "Machine Translation: English." FSA's Supervision Guidelines (URLs subject to change without notice):

Japanese (HTML): <https://www.fsa.go.jp/common/law/guide/kinyushohin/>

Japanese (PDF): <https://www.fsa.go.jp/common/law/guide/kinyushohin.pdf>

English (PDF):

https://www.fsa.go.jp/common/law/guide/kinyushohin_eng.pdf

vi. Systems Planning / Development / Operation and Management

- a) Has a medium- to long-term development plan been formulated with clarification that the system strategy policy is part of management strategy, and has the plan been approved by the board of directors? In addition, has there been strategic investment to identify inherent risks in existing systems and maintain or improve measures?

⁶ Recently, there have been multiple confirmed cases where a trading participant's business operations were hindered (e.g., its trading system was suspended) or its customers incurred losses (e.g., due to the unauthorized withdrawal of their funds) as the result of an unauthorized access (login) to the trading participant's IT system by a malicious third party.

- b) Are there clear rules on approval for planning, development, and migration of development projects, and is project progress being monitored based on the development plan with persons responsible for each project? In addition, have tests been conducted adequately and appropriately (including making test plans and involving user divisions in tests) at the time of system development?
- c) Is there a specific plan to cultivate human resources to ensure continuity and specialized knowledge of existing system structures and development skills?

vii. Systems Audit

- a) Are there periodic audits of computer systems conducted by an internal audit section that is independent from the systems division? In addition, is there internal audit by staff adept at IT systems or external audit by systems auditors? Moreover, are all operations related to IT systems risk covered in the audits? Additionally, are results from the systems audit appropriately reported to the board of directors etc.?

viii. Management of Outsourcing of Business Operations

- a) Are outsourcees (including subsidiary companies and outsourcees through the use of cloud services) determined with evaluation and consideration based on criteria for selection?
- b) Does the financial instruments business operator specify the division of roles and responsibilities, audit authority, sub-contracting process, and level of service provision regarding an outsourcing contract? In addition, does the financial instruments business operator present to the outsourcee the rules or security requirements that officers and employees of the outsourcee should comply with and include the contents in the contract or other documents?
- c) Does the firm perform the risk management of outsourced IT system-related work (including multi-tiered subcontracted work) appropriately? Has it established its risk management system with the full awareness that it would need to perform more sophisticated risk management particularly when it has multiple outsourcees and the management of them has become more complicated? In addition, when the firm outsources IT system-related administrative work, does it perform the same sort of risk management that it performs for outsourced IT system-related work?
- d) Does the financial instruments business operator, as the outsourcer, regularly monitor whether the outsourced operations (including subcontracted operations) are appropriately conducted? In addition, is there an internal management system that allows the outsourcer to monitor and trace the operational status of customer data in the outsourcee?⁷

⁷ With respect to a recent incident of unauthorized withdrawal by an employee of an outsourcee, the unauthorized use of the authority granted to the employee at the outsourcee was disclosed. The financial instruments operator needs to manage outsourcing of business operations by combining the ID management and access restrictions at outsourcees and the monitoring of outsourcees, etc.

ix. Contingency Plan

- a) Is there a contingency plan and a framework for emergency response? In addition, is the plan based on objective levels and does it assume both emergency situations caused by disasters and system malfunctions at the financial instruments business operator that may occur due to internal or external factors? Moreover, have various risk scenarios (including significant delay in batch processing) been considered sufficiently?
- b) Are the assumed scenarios of the contingency plan reviewed appropriately based on cases of system malfunctions at other companies or decisions of the Central Disaster Prevention Council? Are there regular drills based on the contingency plan on a company-wide basis and with outsourcees?
- c) Regarding core systems that are critical for business, is there a management system in place with an off-site backup system, which is prepared in advance to quickly continue business should a disaster or system malfunction occur?

x. Project Management of System Integration Risk

- a) Do officers and employees of the financial instruments business operator fully recognize the risk of system integration, and is there a system to manage such risk? In addition, does the management system allow the financial instruments business operator to be involved objectively even if the operation is outsourced?
- b) Has the financial instruments business operator established arrangements and procedures for conducting tests, and is the test plan suited to the nature of the system development necessitated by the system integration? In addition, does the financial instruments business operator make use of third-party assessments, such as by a systems auditor, when making judgment regarding important matters related to system integration?
- c) Has the financial instruments business operator developed a contingency plan for dealing with unforeseen circumstances?

xi. Response to System Malfunctions

- a) Can appropriate measures be taken to prevent unneeded customer confusion when a malfunction occurs, and are there operations for system recovery or alternative procedures ready for quick implementation? In addition, is there a management system ready to take necessary action, assuming the worst-case scenario in a system malfunction?
- b) In preparing for system malfunctions, etc., is there a clear reporting route or chain of command that includes the outsourcees?
- c) Does the financial instruments business operator immediately report a system failure that has a serious impact on management to the board members including a representative director(s)? Is there a management system to report the maximum risk in the worst-case scenario? (For example, if there is a

possibility that a system failure will have serious impact on customers, the reporter shall be required to report the maximum risk, and not underreport risk based on personal judgment.) In addition, is there a system that makes it possible for the company to establish an emergency headquarters where the representative director and other directors/executive officers can issue instructions to quickly resolve problems?

- d) In the event of a system malfunction etc., has the financial instruments business operator made an announcement with details of the malfunction, its cause, and the expected timing of recovery as well as promptly set up a call center or other department to respond to inquiries from customers as necessary? Moreover, in preparing for system malfunctions etc., have means of providing information to related divisions and information to be provided been clarified?
- e) Has the financial instruments business operator appropriately implemented measures for a system malfunction such as identification of the cause, investigation on the impact until recovery, improvement measures, and measures to prevent a recurrence? In addition, is there regular analysis of trends related to causes for system malfunctions and are there measures to address such trends?
- f) Is there a systematic mechanism such as a failover to minimize the impact of system malfunctions?
- g) Is there a system and framework for prompt reporting to the regulatory authorities when a malfunction occurs?⁸

xii. Other

- a) If external storage media such as USB memory devices are used, are they properly managed?⁹

⁸ System malfunctions, etc. that should be reported (regardless of cause): any malfunction of a system or device (hardware or software) currently in use by a financial instruments business operator, an entity entrusted with operations from a financial instruments business operator, etc., which has or may have impact on financial instruments trading, clearing/settlement, deposit/withdrawal of funds, financing, grasping of financial conditions, or other matters such as customer convenience. However, this excludes cases where no substantial impact occurs due to the prompt switching to other systems/devices even in the event of such impact in some systems/devices (for example, cases where an error in order acceptance systems occurs outside auction trading hours, and prompt switching to alternative systems is completed in time to allow order acceptance during auction trading hours). Furthermore, even when a malfunction has not occurred, reports are required in cases where there is a warning of a cyber-attack or the detection of a cyber-attack, and the possibility of a malfunction like those above is deemed to be high.

⁹ External storage media such as USB memory devices can be a medium for leaking internal confidential information to the outside world, as well as an entry route for malicious software such as viruses. Therefore, it is desirable to reduce the use of such media as much as possible, limit the range of usable media, capacity, and connectable terminals, and implement a control system for checking such devices during and after use.

Reference: Reference materials on IT systems risk are available, such as "FISC Security Guidelines on Computer Systems for Financial Institutions" (published by The Center for Financial Industry Information Systems).

8. Management of Margin Transaction Security Deposit, etc.

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 161-2
- Security Deposit Cabinet Order
- TSE Business Regulations: Rule 14.1.(3) through (6)
- TSE Regulations Regarding Margin Transactions and Loans for Margin Transactions
- TSE Brokerage Agreement Standards: Rule 5, Rule 6, Rules 31 through 40, and Rules 43 through 48

(2) Regulatory Intent and Requirements

Margin trading is a form of securities brokerage in which a financial instruments business operator enters into an agreement ahead of time to loan a customer funds or securities to settle a transaction. In performing a margin transaction, laws and regulations require that the financial instruments firm receive from the customer a security deposit in excess of the amount determined by multiplying the market price of the subject security by a percentage determined by the Prime Minister as necessary for ensuring fairness in transactions.

A "when-issued transaction" is a transaction for a security that has yet to be issued. On the settlement day, a certain amount of time after the issue date, the subject security is delivered and, as with margin trading, it is necessary to receive a security deposit from the customer.

An amendment, effective January 1, 2013, was made to change calculation and valuation of customer margin pertaining to margin transactions from the delivery date to the contract date. Prior to this, 30% of customer margin for unsettled positions was not to be withdrawn until the delivery date. Following this amendment, it is possible to release withholding from customer margin pertaining to positions for which settlement has been declared. Additionally, before the amendment, the amount available for immediate allocation was limited to once per day for only offsetting transactions. With the amendment, such immediate allocation as customer margin for other margin transactions is possible multiple times, regardless of method of settlement. However, if new positions/settlements are repeatedly conducted (day trading) without the deposit of customer margin (including cases of insufficient customer margin), the deposit of customer margin for all transactions is required.

Additionally, prior to the amendment, withdrawal and allocation of fixed profits was only possible on or after the delivery date of such offsetting transaction. However, after the amendment, such profits can be included in the total amount of customer margin immediately after offsetting transactions.

Furthermore, the amendment was also made to additional margin. Previously, when additional margin was required, the deposit of cash or securities in lieu of cash was required. Following the amendment, (1) in cases of partial settlement of a position, deduction of 20% of such from the additional margin, and (2) in cases where advanced deposit of fixed losses

was conducted, deduction of such deposit from the additional margin is permitted.

In addition, the following points should be noted:

- i. When a sale or purchase is made through a margin transaction, the customer margin – equal to 30% of the execution price (and no less than JPY 300,000) – must be deposited by the customer by a date and time specified by the trading participant by noon of the second day following the execution date (T+2).
- ii. Cash or securities may be withdrawn from those deposited as customer margin equivalent to the amount equal to "30% of the contract price of all securities pertaining to margin transactions (excluding those used for settlement)" subtracted from the "total amount of such customer margin".
- iii. When a trading participant, on its own, has imposed margin terms and conditions (for example, a higher minimum margin, tighter deadline for deposit of security deposit, higher credit limit, regulations on nikai-date transactions (a transaction in which an issue purchased on margin is the same as an issue being used in lieu of money as the margin deposit, etc.) for margin transactions and when-issued transactions that are stricter than those required by laws and regulations, it must explain said terms and conditions to the customer ahead of time and gain its sufficient acceptance.
- iv. At internet securities firms using margin accounts to centrally manage funds for customers' margin transactions, there have been an unduly large number of violations of net settlement transaction and same-day cash collection regulations for cash transactions funded with margin funds. A trading participant taking this approach, therefore, must be sure to comply with not only margin transaction regulations but all net settlement transaction and all other closely related regulations, as well.
- v. The security deposit rate for margin transactions of ETFs and ETNs tracking leveraged and inverse products will be that obtained by multiplying 30% by the leverage factor of the relevant product. (If the leverage factor is negative, the rate will be obtained by multiplying 30% by the value obtained by deducting the leverage factor of the relevant product from zero.)

(3) Key Management Checkpoints

- i. Have appropriate organizational measures been taken to manage security deposit and other matters related to margin and when-issued transactions?
- ii. Have internal rules (internal regulations or operating rules) been properly established to manage security deposit (including measures addressing regulations for increasing margin and regulations concerning cash) related to margin and when-issued transactions?

- iii. In cases of response to the deregulation that was enforced on January 1, 2013, has an appropriate internal management system, including post factum inspection, been established?
- iv. Do the head office's compliance division and each branch office respectively perform searches for accounts, etc. for which margin falls short of either the 30% initial margin requirement or the 20% maintenance margin requirement, or accounts that may potentially fall into such a situation?
- v. Have approaches (integrated internal processing flow or penalties) for dealing with additional margin calls and improper withdrawal of margin funds been established within the firm and are they being uniformly applied?
- vi. Have operational measures (internal communications, customer notification, or compliance checks) been taken that would allow actions pursuant to margin-increase and cash regulations concerning margin transactions?
- vii. Have internal systems been established to check and archive the Agreement for Setting up Margin Transaction Account and the Agreement on Entrustment of When-Issued Transactions? Have internal systems been also established to deal with revisions to these agreements?
- viii. As a precaution, are measures for forcibly locking customer accounts in place and implementable if they are required?
- ix. For accounts nearing the settlement deadline, are management measures for issuing notifications in place? In addition, are measures in place that would allow responsible employees to take proper actions for dealing with customers and other purposes, as well?
- x. Has an internal system been established (e.g., coordination between the compliance division at the head office and the sales departments at the head and branch offices) for cases when an employee cannot decide whether a customer is allowed to make a margin withdrawal during a transaction?
- xi. Have decision criteria for the correction of margin trading classification information (for example, correction to new margin purchase from cash purchase) reported to TSE been properly established and are they being applied under uniform internal procedural flow?
- xii. Has training for managing margin and when-issued transactions been developed?
- xiii. How does the firm warn customers to comply with rules on margin withdrawal and other rules on margin transactions and when-issued transactions (both laws, rules, and regulations as well as the firm's own rules)? For example, does it post warnings on its website or contact individual customers?

9. Error Correction Management (Correcting the Own-Account/Customer-Account Classification and Errors)

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 39.3 through 5
- FIB Cabinet Order: Articles 118 through 122
- TSE Business Regulations: Rule 14.1.(1) and Rule 41
- OSE Business Regulations: Rule 26.1 and Rule 34
- JSDA: Regulations Concerning Application for Confirmation and Examination, etc. of Incidents, others

(2) Regulatory Intent and Requirements

While it would be best if securities transaction errors or incidents (hereinafter "incidents") were simply not committed, it is, in reality, impossible to completely eliminate them. Execution corrections are used as one way to protect customers from losses resulting from a wide range of incidents, including simple administrative mistakes in order execution. However, because of the ample possibility of loss compensation, provision of undo gains, and other illegal activity under the guise of execution correction, the FIEA requires that a confirmation be provided to the Prime Minister before any losses are borne in connection with the correction of a customer order and that a report be filed after losses are borne.

FIB Cabinet Order Article 118 enumerates five types of incidents. These are: 1) an unconfirmed trade; 2) mistaken solicitation; 3) an error in executing a customer order caused by an administrative mistake resulting from negligence; 4) an error in executing a customer order caused by an abnormality in an electronic information processing system; and 5) activity that violates other laws and regulations.

Execution correction is said to directly reflect compliance awareness and internal management readiness to act at financial instruments business operators, but, depending on how corrections are handled, may also serve as a breeding ground for improper or illegal activity. That makes it an extremely important area for compliance. Among the wide variety of execution correction approaches, JPX-R inspections, noting the close relationship with exchange trading, focus in particular on corrections made to the own-account/customer-account classification¹⁰ and error correction¹¹ in examining the propriety of correction details and management of correction procedures.

In addition, the following points should be noted:

- i. The FIB Cabinet Order provisions on negligence-caused administrative errors in customer order execution apply to administrative mistakes between the receipt

¹⁰ When placing an order on TSE or OSE, a trading participant must specify whether the order is for its own account or for that of a customer and, if later correcting that specification, must provide a Corrected Declaration to TSE or OSE.

¹¹ With the approval of TSE or OSE, a trading participant can execute an order intended to correct an error in a customer order outside of a trading session.

of an order and order execution. Not included are improprieties at the time an order is received (for example, an unconfirmed trade or mistaken solicitation) and administrative errors after execution ("execution notification mistakes").

- ii. Correction of administrative errors that occur up through the day preceding delivery do not require confirmation of an incident as the customer is not considered to have actually suffered a loss due to a mistake. (Note: Reissuance of the order and other corrective actions, however, are required.) It is important to note that, with respect to unconfirmed trades or mistaken solicitation, changing to its own account is prohibited, even before delivery.
- iii. To prevent a trading participant from assigning to a customer account, after the fact, a transaction undertaken for its own account, or compensating a customer for loss on its account by reassigning the transaction to the participant's account, both TSE and OSE require that orders be classified by trading participants as for their own accounts or for customer accounts when they are placed. Changing the classification after the fact is permitted only when correcting an administrative error.
- iv. Business Regulations of TSE and OSE prescribe that a trading participant may execute a sale or a purchase of a security without carrying out a trade during a trading session (a transaction for correcting errors) with the trading participant as a counterparty, when the trading participant has placed the erroneous order due to an error, etc. for a truly unavoidable reason or due to a computer system malfunction.

Similarly, subject to certain conditions, a trading participant may apply for error correction when a trading participant is unable to execute an order of its customer in accordance with the purpose of entrustment in the TSE or OSE market in accordance with the purport of the entrustment due to an unavoidable error caused by the staff other than traders of the trading participant (such as sales staff).

(3) Key Management Checkpoints

- i. Execution Correction in General
 - a) Have internal rules (internal regulations or operating rules) been properly established for correcting incidents?
 - b) Has a unit and a person-in-charge been designated for rendering final judgment on the adequacy of an execution correction application? (Have there been cases in which action was taken in contradiction to the decision of said person?)
 - c) Have procedures spanning the period from incident emergence through correction application been developed, and is it possible to implement them smoothly and uniformly?
 - d) Have supervising units taken steps, like keeping ledgers, using voice recorders,

and arranging for direct confirmations with customers, which permit the confirmation of facts for error reports (internal correction rationale documentation) and other purposes, should an incident arise?

- e) Has it been determined what units and personnel will prepare corrected declarations to the exchange and perform overall checks, and has a system allowing all of the parties to contact one another been established?
- f) Are reports on execution correction results regularly provided to those in charge of internal management? For particularly important cases, are reports made promptly after the incident takes place?
- g) When there are concerns regarding the processing of an execution correction or for particularly significant incidents, is there a system in place for consulting with a self-regulatory organization and other parties before going through with correction procedures?
- h) Have proper measures (including retraining) been taken with regard to personnel who have frequently made errors?
- i) Does the error report (internal correction rationale documentation) include information such as supporting documentation on circumstances surrounding errors, causes, specifics of correction steps, and proof of facts that would permit checks to be performed? In addition, are error reports and related documentation properly filed by supervising or other units?

ii. Own-Account/Customer-Account Correction

- a) Has the system been configured so that the own-account/customer-account classification is automatically recognized (automatic setting of the classification either by terminal or by inputting a customer code)? If the system does not automatically set the classification, are checks performed appropriately to determine whether the classification has been input appropriately?
- b) Are supervising units appropriately examining correction rationale to determine whether gains have been transferred to customers by re-classifying an own-account transaction as a customer-account transaction and whether losses have been transferred to the firm by re-classifying a customer-account transaction as an own-account transaction?
- c) Were the documents submitted for correction to TSE or OSE double checked both in formality and content by those in charge of or involved in the transaction?
- d) Have criteria been clarified for determining whether it is possible to reclassify a transaction as an own-account transaction in the case of an execution correction after the settlement date?

- e) For the processing of extremely large orders, are consistent, rational rules applied in reclassifying orders as own-account orders?

iii. Error Correction

- a) Are internal rules, notifications from exchanges, and other documentation related to error correction all retained?
- b) When an Application for Correction is to be submitted to TSE or OSE, are double checks of the submitted documents performed in formality and content by those in charge of and involved in the transaction?
- c) How do the internal control units check that they are applying for correction for a "truly unavoidable reason" prescribed in the rules of TSE or OSE? For example, do they use records taken with voice recorders, or do they use other measures?
- d) Are measures in place to properly perform checks to determine the authenticity of documentation such as order slips attached to Corrected Declarations?

10. Compliance with Same-Day Cash Collection Rules

(1) Relevant Laws, Rules, and Regulations

- TSE Business Regulations: Rule 65
- TSE Rules on Regulatory Measures Concerning Securities Trading or Its Brokerage: Rule 1.1.(7) and (8), others

(2) Regulatory Intent and Requirements

When TSE determines that the state of securities trading on the exchange has become abnormal or is likely to become so, it will take the necessary measures provided in TSE's rules. Regarding the determination of initial prices for initial listings, these rules include regulations for requiring payment of purchase money prior to settlement—in other words, the same-day collection of cash for transactions.

In addition, when these regulations are applied, TSE may also apply regulations prohibiting trading participants involved in trading for the purpose of determining initial price from making purchases for their own account (including purchases pursuant to discretionary trading agreements).¹²

Same-day cash collection regulations, it should be noted, can also be implemented with regard to trading in issues already listed.

In addition, the following points should be noted:

- Same-day cash collection regulations apply not only to the exact time when an initial price is determined but through the end of that day.
- "Cash" includes:
 - Cash
 - Drafts
 - Customer deposit account funds used as purchase money
 - MRF (Money Reserve Fund) exceeding amounts necessary as purchase money for other transactions and that is applied as purchase money for the transaction to which same-day collection regulations are being applied
- Margin transactions are not exceptions to same-day collection regulations, so, for margin transactions involving the same issue, same-day collection of cash equivalent to the purchase money amount is required in addition to the deposit of security deposit.

¹² Prior to the amendment, the regulation prohibiting market sell orders related to trading up through the day the initial price is determined was also applied. However, for newly listed issues since June 26, 2023, both market bids and offers related to trading on the initial listing date (or until the day the initial price is determined if the initial price was not determined on the initial listing date) have been prohibited.

(3) Key Management Checkpoints

- i. Have manuals on securities trading regulatory measures been prepared? In addition, have notifications from exchanges (including self-regulatory organizations) and other such information been properly organized and archived?
- ii. When regulatory measures are announced by TSE, do relevant personnel review details and properly inform personnel involved in operations?
- iii. Are measures appropriately taken to provide information on newly announced regulatory measures to customers from whom orders were received prior to the announcement, internet customers, other financial instruments business operators from whom orders can be received online, and other customers?
- iv. To ensure the same-day collection of purchase money, are appropriate management, including systems-based, steps (to ensure prior receipt of all purchase money) taken when an order is received from a customer for an issue subject to regulatory measures?
- v. Are management procedures (including checks by sales offices and the head office to determine whether purchase money has been received) for execution days for issues subject to regulatory measures properly performed?
- vi. Are management procedures properly performed on a daily basis until the delivery date to ensure that purchase money that is supposed to be locked up is not used for other purposes or withdrawn?
- vii. Are internal inspections and examinations performed to ensure compliance with the subject regulatory measures? If they are, what do they focus on and with what frequency are they being performed?

11. Measures to Prevent Erroneous Orders

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 40.1.(2)
- FIB Cabinet Order: Article 123.1.(14)
- TSE Trading Participant Regulations: Rule 22-3 and Rule 42
- OSE Trading Participant Regulations: Rule 21-2 and Rule 51
- TSE Rules concerning Order Management Systems at Trading Participants
- OSE Rules Concerning Order Management Systems at Trading Participants
- TSE/OSE/JPX-R Order Management Guidelines

(2) Regulatory Intent and Requirements

Placement of an erroneous order is a prime example of administrative risk, so prevention is a key compliance issue for financial instruments business operators. Individual trading participants, therefore, have long worked to prevent the placement of erroneous orders by employing limit controls in their systems and taking management measures to ensure employees are as accurate as possible in entering orders. Even so, however, it has been impossible to root out the placement of erroneous orders, which has a considerable impact on exchanges.

In December 2005, placement of a massive erroneous order resulted in a transaction for shares significantly beyond the total number of issued outstanding shares for the issue, and the impossibility of ordinary settlement by delivery and payment procedures necessitated an extremely serious situation in which settlement had to be made in cash. In such cases, where the placement of a large erroneous order has a tremendous impact on the market, the negative consequences are not limited to the immediate loss incurred but extend to administrative disciplinary action and disciplinary action by self-regulatory organizations.

Learning from this experience, TSE and OSE established its "Rules concerning Order Management Systems at Trading Participants" in 2006 and now require all trading participants to have appropriate systems in place to prevent the placement of erroneous orders.

In recent years, the market has experienced the ever-growing prevalence of trading through electronic data processing systems that automatically place orders. Given concerns over the impact on the markets caused by malfunctions in electronic data processing systems, it is increasingly important for trading participants to develop an effective system for order management. As such, in April 2018, exchanges clarified certain aspects surrounding order management in the rules such as by establishing limits to prevent order placement for which the total quantity or amount of orders at a certain time exceeds a certain quantity or amount, among other things. These include, in addition to limitation on one-shot order placement, order management that is deemed to be appropriate for preventing the misplacement of an excessive quantity of or monetary amount for many small orders.

Furthermore, in accordance with the introduction of the Market Access Rules in January 2021, trading participants are required to implement direct and exclusive risk controls,¹³ restrict the placement of subsequent orders after an erroneous order has been placed, and clearly prohibited deliberate erroneous orders (e.g., Malformed Order) from the standpoint of enhancing risk check functions by trading participants, among other things.

In addition, the following points should be noted:

- i. The Rules concerning Order Management Systems at Trading Participants (hereinafter "Erroneous Order Management Regulations") require the establishment of order management systems for all the products listed on TSE and OSE, for which trading participants can place orders, regardless of their order placement frequency.¹⁴ Therefore, for example, even if a trading participant rarely handles orders for certain listed products, it will be in violation of the Erroneous Order Management Regulations if it fails to act in accordance with the Erroneous Order Management Regulations.
- ii. The purpose of the Erroneous Order Management Regulations is to prevent the receipt and issuance of erroneous orders by trading participants. "Erroneous orders" here includes orders that are erroneous because of customer mistakes. Consequently, proper management based on the same regulations is required for customer orders received via the internet or Direct Market Access (DMA) (hereinafter collectively referred to as "orders received via the internet")
- iii. The Erroneous Order Management Regulations require the establishment of soft limits to allow trading participants to eliminate erroneous orders. It is necessary to avoid allowing the person responsible for approvals related to soft limits (hereinafter "soft limit approver") to grant approvals for his or her own orders when they exceed a soft limit. For an order exceeding the soft limit, a double check by a person other than the person making the order is necessary to avoid placement of an erroneous order. In other words, a person to whom authority has been delegated by the soft limit approver or another internal person with soft limit approval authority must check the order details and determine whether to grant approval.
- iv. For orders received via the internet, it is conceivable that soft limits could be applied in the order placement systems used by customers. Doing so would require the display of a warning screen and proper use of the limit release method to avoid the placement of erroneous orders arising from the customer's release of the limit without adequate understanding.
- v. A "hard limit" must be set at a level at which there is essentially no possibility of a legitimate order being made, while a "soft limit" must be set at a level at which

¹³ "Direct and exclusive risk control" means a situation where only the trading participant can manage restrictions or measures related to order management of customers (for example, setting, change, etc., of risk parameters) and where the customers cannot modify such parameters, etc.

¹⁴ Regulations of TSE and OSE apply specifically to auction trading, but it goes without saying that using these regulations as a guide for setting hard limits for off-auction trading (ToSTNeT trading and J-NET trading) and taking other appropriate internal management steps is desirable.

legitimate orders are not usually made but at which they may occasionally be made. These levels differ depending on the transaction circumstances of individual trading participants, so it is necessary for individual trading participants to consider carefully where to set these levels and then set them at levels appropriate for their operations. Particularly, hard limits need to be set within the order size limits specified by TSE and OSE.

- vi. For example, let us assume that (i) an order significantly exceeds the trading participant's past order activity, or (ii) the hard limit does not function for a trade, because it was set for off-auction trading, and an order exceeds the order size limits set by TSE and OSE for auction trading. In such cases, where no effective limits are set from an objective viewpoint, the trading participant will be deemed to have not set appropriate order limits and have failed to comply with the Erroneous Order Management Regulations. Therefore, trading participants are required to pay attention to the following matters, among others: (i) whether concrete limits are set at levels that are comparable with past order activity, (ii) whether the limits are set at all terminals that have order placement functions, and (iii) whether limits set by the trading participants are within the order size limits that TSE and OSE have specified by product and by market segment.

It should be noted that, while it would be difficult to say that setting a hard limit at a level appropriate for a soft limit and managing orders with only a hard limit violates the Erroneous Order Management Regulations, hard limits must be appropriately (conservatively) set in a manner that is not excessive.

- vii. Regarding a soft limit, it can be said that what constitutes an appropriate level can change depending on market conditions. The effectiveness of a soft limit, therefore, can be seen as dependent on changing its level appropriately. In the case of a hard limit, on the other hand, the level at which there is essentially no possibility of legitimate orders is not expected to change frequently in response to market conditions, so more care must be applied in changing the level of a hard limit.
- viii. Hard limits and soft limits must be set for all terminals from which it is possible to place an order on the TSE and OSE market. This includes, for example, TSE terminals ("exchange terminals") that could be used at the time of a system malfunction, and not just those normally used in daily operations.
- ix. For orders received from customers via the internet, creating a system that does not permit orders exceeding certain levels for funds and securities deposited by customers (hereinafter "advance receipt system") and using this system as a hard limit leaves open the possibility that a level at which there is essentially no possibility of legitimate orders will be exceeded. Consequently, the establishment of an advance receipt system does not necessarily mean that a hard limit is unnecessary.

Furthermore, for systems in which orders are limited based on the assessed values of securities deposited by customers (hereinafter "deposited assets valuation system") and other systems in which a full-scale advance receipt system is not being used, it is even more necessary to establish a separate hard limit, and to carefully consider the sizes of the orders that customers could

actually place.

- x. Regardless of whether a trading participant accepts orders for low latency trading, in the event that an unexpected irregular order was placed due to a malfunction, etc. of the order placement system (including customer systems), the trading participant is required to immediately implement measures to deter placement of new orders to the exchanges.¹⁵

(3) Key Management Checkpoints

- i. Have internal rules (internal regulations or operating rules) been properly established in conformance with TSE/OSE regulations to prevent the placement of erroneous orders?
- ii. Has a system been established (i.e., a unit and the staff that are responsible) for comprehensively grasping the status of the order limit settings (the settings of each hard and soft limit) for the in-house order placement system?
- iii. Are checks performed appropriately to determine whether a terminal's order limits have actually been set as stipulated in the rules and if they have been set at appropriate levels? In addition, are checks performed appropriately to see if the hard limits for orders that are placed using said terminal have been set within the exchanges' order size limits (compared to the order size limit that has been established individually by product and by market segment)?
- iv. Have internal procedures for changing order limits been clearly established, and are operations being performed appropriately based on those procedures?
- v. When an order is received from a customer, how are order details and financial means confirmed to prevent placement of an erroneous order? Are these steps properly taken for wholesale, retail, internet, call, DMA, and other transaction routes (order systems)?
- vi. Particularly with respect to conducting trades involving automatic order placement using algorithms, etc. (including proprietary trading), has a proper management system (cumulative position limits, etc.) been established to address the inherent risks to this transaction type, such as the risk of placing large amounts of irregular orders due to a trading system failure, etc., which may lead to immense losses directly connected to the bankruptcy of clients, etc., as well as the likelihood of significantly impacting the operations of exchange markets?
- vii. Does the trading participant ensure that the following situation does not occur: the

¹⁵ Trading participants that accept orders for low latency trading continue to be required to implement measures based on checklists requested by the TSE Equity Strategic Planning No. 300 notice dated Nov. 26, 2018 and the OSE Market Planning No. 19 notice dated Mar. 29, 2019.

placement of an order that has violated the trading participant's order limits but has been intentionally modified so that it would clearly cause an error and be rejected by the exchange's system instead (i.e., the placement of a malformed order)?

- viii. Have system settings and management structures been established so that, when an irregular order is placed, no further orders can be placed to the exchanges? In addition, has the handling of unexecuted orders (still on the exchange's order book) when no further orders can be placed been considered in advance?
- ix. Does the trading participant have direct and exclusive control over setting and modifying order restrictions and order suppression when an irregular order has been placed, etc.
- x. Have concrete procedures for releasing soft limits been established, and are they consistently followed? In particular, in the case of order placement by someone with release authority, is release of such limits or order entry subject to checks by another person?
- xi. Are soft limit levels revised at appropriate times and in appropriate ways given transaction circumstances? Have high soft limit levels, set when market conditions warranted them, ever been left in place even though lower levels were called for?
- xii. Do personnel in charge of placing orders correctly understand and implement operations and procedures to prevent placement of erroneous orders?
- xiii. Have units responsible for placing orders deployed personnel appropriately and do they properly conduct training to prevent placement of erroneous orders?
- xiv. Does training incorporate how to address warning notices and perform cancellation procedures?
- xv. Have proper measures (including retraining) been taken with regard to personnel who have frequently made entry mistakes?
- xvi. Have basic response policies and an internal reporting system been put in place to handle the placement of large erroneous orders? In addition, has a specific contingency plan been developed to permit appropriate responses?
- xvii. Have information disclosure policies and specific disclosure methods been properly established to deal with the placement of large erroneous orders?
- xviii. When the trading participant offers a new product, adds a product to its lineup, or replaces its systems, does it set the necessary order limits?
- xiv. Does the trading participant also restrict order placement entrusted by customers from other financial instruments business operators?

12. Trading Supervision Systems

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 40.1.(2)
- FIB Cabinet Order: Article 123.1.(12), others
- TSE Trading Participant Regulations: Rule 22-2
- TSE Rules concerning Trading Supervision Systems at Trading Participants to Prevent Unfair Trading
- TSE Guidelines for Rules concerning Trading Supervision Systems at Trading Participants to Prevent Unfair Trading
- OSE Trading Participant Regulations: Rule 21
- OSE Rules concerning Trading Supervision Systems at Trading Participants to Prevent Unfair Trading
- OSE Guidelines for Rules concerning Trading Supervision Systems at Trading Participants to Prevent Unfair Trading

(2) Regulatory Intent and Requirements

In light of such factors as an increase in non-in-person trading, TSE requires trading participants to establish trading supervision systems in order to prevent unfair trading, ensure investor confidence in TSE's markets and in trading participants, and protect the public interest and investors. Specifically, TSE has stipulated in its regulations what trading participants are required to do in order to establish trading supervision systems for securities (stocks, convertible bonds (CBs), exchange-traded funds (ETFs), other) on TSE's markets. In short, trading participants are required to: 1) establish internal rules that prescribe matters concerning the accurate understanding of trends in customers' trading; 2) conduct trade surveillance through searches for specific issues and customers; 3) prepare and retain internal records; and 4) address other matters.

These regulations (implemented in June 2006) originally targeted unfair trading by customers but were later amended (amendments implemented in December 2007) to require the establishment of trading supervision systems covering trading participants' trading for their own accounts. In addition, in April 2020, OSE's Rules concerning Trading Supervision Systems at Trading Participants to Prevent Unfair Trading were implemented to specify the trading supervision systems required for market derivatives transactions. In April 2022, TSE's Rules concerning Trading Supervision Systems at Trading Participants to Prevent Unfair Trading were revised to more flexibly allow trading participants to modify search criteria and matters concerning analysis, and requirements for trading participants conducting principles-based trade surveillance were clarified in the guidelines for these Rules.

TSE and OSE regulations set forth the minimum standard for appropriate transaction-monitoring systems required of trading participants by FIB Cabinet Order Article 123.1.(12). Individual trading participants, therefore, should go beyond compliance with these minimum requirements (for both in-person and non-in-person, and wholesale and retail

trading) to take additional steps appropriate for their own circumstances to achieve even higher compliance levels. Trading participants need to provide the designated reports with the Trading Participants Office at either TSE or OSE every time internal rules that comprise the operational standards for trading supervision systems are changed.

(3) Key Management Checkpoints

- i. Does the content of the internal rules (on trading supervision to prevent unfair trading) fulfill the requirements of the exchange regulations? In addition, have operating manuals been properly prepared, so that trade surveillance can be smoothly carried out on a daily basis?
- ii. Are internal rules and the performance of trade surveillance activities appropriately examined and revised in light of actual trading circumstances?
- iii. Have communications and reporting systems been properly established between trading supervision units and branch offices? In addition, are trading supervision units properly providing instructions and advice?
- iv. In daily trade surveillance operations, are searches for customers being conducted appropriately based on search criteria that conform to the exchanges' rules? In particular, does the trading participant ensure that the following situation does not occur: a situation in which the trading participant conducts a search for a transaction that is subject to trade surveillance without realizing that some of the information pertaining to the transaction was not incorporated into the trading participant's trade surveillance system?¹⁶ In addition, does the trading participant ensure that the following situation does not occur: transactions that should be included in a search are missing from the search due to such reasons as an error in the trade surveillance system's search logic?¹⁷
- v. Is trade surveillance conducted appropriately on the transactions and customers that were found based on search criteria that conform to the exchanges' rules?¹⁸

¹⁶ A trading participant is required to conduct appropriate trade surveillance of market derivatives transactions in consideration of such factors as its customers' forms of trading. However, depending on such circumstances as its trading volume, the trading participant may choose to conduct trade surveillance based on such information as trading data or order slips rather than searching for transactions in its trading system.

¹⁷ While one must handle situations where transactions that should be included in a search are missing from the search, in order to conduct trade surveillance efficiently, one must also appropriately handle situations where too many transactions are being included. For example, in the case of a trading participant that brokers orders from many originating customers via its overseas affiliates, if all of the customers of the overseas affiliates are included in the search, then the transactions of multiple irrelevant originating customers will be searched for. By using search settings that match their customer attributes and trading circumstances and efficiently searching for the necessary transactions, JPX-R believes that trading participants will be able to conduct in-depth trade surveillance as a result.

¹⁸ Does the trading participant conduct trade surveillance of market derivatives transactions

Particularly when a large number of cases are searched for each day, does the trading participant ensure that the following situation does not occur: in order to reduce the number of cases subject to trade surveillance, the trading participant rashly narrows the search using an arbitrary criterion (e.g., involvement ratio, price change)?¹⁹²⁰

- vi. Are the "Guidelines Concerning the Trading of Issues Subject to Additional Financing" published by JPX-R being properly applied in supervising the trading of issues subject to additional financing?
- vii. Is the work pertaining to a listed company's acquisition of its own shares, including information management and transaction execution (brokerage of the purchase), handled appropriately based on laws and regulations as well as JPX-R's "Guidelines Concerning the Acquisition of Own Shares"?
- viii. Is trading surveillance related to information disclosed by listed companies being performed properly with regard to trading by registered insiders?
- ix. Are trading supervision and trade surveillance conducted appropriately with regard to non-trading participants and to customers who trade via DMA?
- x. Have appropriate measures for the issuance of cautions to customers and other

appropriately in accordance with such factors as its customers' forms of trading (e.g., the characteristics of the products in its lineup; the attributes, trading volume, and order placement methods of its customers)? (Please note that in light of past cases in which monetary penalties were imposed on trading participants, particular attention must be paid to spoofing and cross transactions.)

¹⁹ No objections will be made to such actions as changes to the search criteria (changing the search criteria or narrowing down the search results) as long as they are reasonable criteria that can obtain surveillance results that are similar to the results of surveillance conducted on customers found using search criteria that conform to TSE's rules. As an example of a reasonable method of narrowing down search results, if a customer has made similar transactions and they have been found in large quantities daily using the same search item, and the trading participant has a detailed understanding of the contents of the transactions and the trading strategies behind them and, as a result of its trade surveillance of the customer, it has determined that there is an extremely low possibility that the customer engaged in unfair trading, then it may switch to using a sampling survey for any subsequent surveillance. (Please note that when changes to the search criteria have been made, JPX-R will verify during its trading participant inspection whether the changed criteria can obtain surveillance results that are similar to those obtained using search criteria based on TSE's rules, after taking into consideration such factors as customers' forms of trading.)

²⁰ If a trading participant conducts principles-based trade surveillance as prescribed in Rule 4.1.(1).c. of TSE's Rules concerning Trading Supervision Systems at Trading Participants to Prevent Unfair Trading, JPX-R will verify whether it has established a trading supervision system in consideration of such aspects as its business conditions and customer attributes and in accordance with the likelihood of an occurrence of unfair trading as well as whether a system is adequately established and functioning to ensure that the trading supervision system has a certain level of effectiveness.

actions been properly established based on trade surveillance results? In particular, are effective measures being taken toward customers based on careful examinations of trading activities, and not simply as mechanical, administrative responses?

- xi. Have appropriate measures (re-examination, etc.) been taken after being cautioned ²¹ by JPX-R Market Surveillance and Compliance Department regarding the possibility of illegal trading?
- xii. Is a system in place for immediately reporting to TSE (JPX-R Market Surveillance and Compliance Department) and other authorities of possible insider trading indicated by trade surveillance results?
- xiii. Are trade surveillance records being properly prepared and retained in accordance with internal rules? In addition, have the contents of the records become effective in terms of subsequent trade surveillance or measures to customers?
- xiv. Regarding trading for the firm's own account and in the derivatives market, is trading supervision being properly performed in light of actual trading circumstances?
- xv. Regarding internal rules and other relevant matters, is training performed at times and in ways that promote the establishment of trading supervision systems for preventing unfair trading?
- xvi. In spoofing surveillance, are unexecuted orders that have been partially cancelled also subject to search?
- xvii. In spoofing surveillance, does the firm perform trade surveillance that takes into account a trade's overall impact on the order book's status, such as by confirming that the pattern of order placement is not multilayered, rather than immediately determining the trade to be acceptable based on the quantities of the individual orders?
- xviii. Considering their impact on price formation in the market, does the firm conduct surveillance on imbalanced cross trades (i.e., the execution of a trade where the quantity to be sold differs from the quantity to be bought) by the same investor? Is a cross trade readily determined to be acceptable merely because its purpose is to extend the settlement date of a margin transaction or to raise funds for the seller?
- xix. If the firm conducts principles-based trade surveillance (with respect to Rule 4.1.(1).c. of TSE's Rules concerning Trading Supervision Systems at Trading

²¹ JPX-R will provide an explanation regarding a particular transaction to a trading participant's person responsible for or in charge of trade surveillance and trade monitoring in order to provide early warning if, for example, the order placement and execution patterns of a particular client are deemed likely to lead to a future violation if left unchecked.

Participants to Prevent Unfair Trading), are the firm's management systems for design, implementation, quality control, and feedback established and operational, and has the effectiveness of the firm's trading supervision system been ensured?

Reference 1: "Event Screening" and Proprietary Trade Surveillance for the Prevention of Unfair Trading

In 2022, there was a case of market manipulation in a trading participant's proprietary trading, and the trading participant's event screening and its proprietary trade surveillance system were deemed to be insufficient.

The following is a summary of the status of event screening and proprietary trading supervision at the trading participants who responded to JPX-R's survey. Trading participants are expected to use this summary as a reference while taking into account such factors as their business conditions, business activities, and customer attributes. If they find any items that they are not sufficiently screening/surveilling or items that would be useful to screen/surveil in order to more appropriately conduct trading supervision to prevent unfair trading, they are encouraged to consider them and make the appropriate revisions.

(1) Status of Event Screening

Event screening refers to the trade surveillance that a trading participant conducts by searching for transactions that were made following such events as "financing" or "block trades"*, knowing that the risk of specific types of unfair trading increases following the occurrence of such events. Event screening is conducted separately from the rules-based search/surveillance that is based on JSDA's and the exchanges' rules.

* Financing, stabilization (those permitted by laws and regulations), syndicate cover transactions, IPOs, the purchase of moving strike convertible bonds (MSCBs), a listed company's acquisition of its own shares, closing price guaranteed transactions, index rebalancing, events related to barrier options such as exchangeable bonds (EBs), block trades (where the buyer also conducts block trades), block offers (where there are many buyers), off-auction distribution, the release of analyst reports, the end of the fiscal year (issues entering a grace period for delisting), etc.

(2) Status of Proprietary Trading Supervision

As a means to improve their management systems to prevent the occurrence of unfair trading, some trading participants are making efforts to conduct trade surveillance not only with the rules-based search criteria and analysis that applies to brokerage trading but also with stricter search criteria in proportion to their proprietary trading status.

In addition, as the nature of each trading participant's business changes, the contents of their proprietary trading also changes, and the risk of unfair trading changes accordingly. In order to respond promptly to this, some trading participants are making efforts to analyze and evaluate their proprietary trading and the status of their proprietary trading supervision and to make revisions (regularly and when necessary) when appropriate.

Reference 2: Trade Surveillance of Spoofing in Market Derivatives Transactions

Recently, acts of market manipulation through spoofing involving multilayered order placement/cancellations or corrections to prices that are less favorable than the best execution price (hereinafter “multilayered order placement/cancellations, etc.”) have been repeatedly observed in market derivatives transactions. The following issues have been observed in trading participants’ trading supervision systems: (1) trade surveillance that does not sufficiently take multilayered order placement/cancellations, etc. into account and (2) an insufficient consideration of a reasonable search threshold for transactions that are subject to trade surveillance, and the absence of a spoofing-related threshold that is tailored to the firm’s trading conditions.

Because of this, JPX-R has provided trading participants with information on (i) methods of searching for multilayered order placement/cancellations, etc., and (ii) examples of best practices for considering reasonable thresholds. For further details, please refer to “II. Trade Surveillance of Spoofing in Market Derivatives Transactions” of JPX-R Trading Participants Examination & Inspection Dept. Notice No. 5 and TOCOM Self-Regulation Dept. Notice No. 4 “Regarding the Collection of Case Studies of Examination Results for Q3 FY2025” (dated Jan. 19, 2026).

In future examinations and inspections, JPX-R plans to gain a detailed understanding of each firm’s management practices and, when needed, provide guidance and advice on improving them. Therefore, JPX-R would like to ask each firm to refer to the best practices, etc., confirm the firm’s search methods and thresholds, and revise them when needed.

13. Management of Margins for Futures and Options Trading

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 119
- Cabinet Office Order on Financial Instruments Exchanges: Article 64, others
- OSE Rules on Margin and Transfer of Unsettled Contracts Pertaining to Futures/Options Trading
- JSCC Rules on Margins, etc. for Futures and Options Contracts

(2) Regulatory Intent and Requirements

When engaging in futures or options trading in the exchange market, customers must make a margin deposit with the trading participant by the day following the day of the transaction. (Non-residents must make margin deposits by the second day following a transaction; hereinafter the same.)

Margins deposited with trading participants are deposited with JSCC as clearing margin (via JSCC clearing participants).

Where a customer deposits customer margin with a trading participant, the trading participant may substitute its own funds or securities, etc. with margins deposited by the customer to make deposits (replacement deposits) at JSCC.

In the case where a trading participant trades commodity futures and options at OSE, the trading participant is required to establish a system for managing such trades, taking into account matters unique to commodity futures and options required to be addressed, such as security deposit receipts and delivery clearing margin.

This section describes handling by OSE. Some rules differ with respect to handling by Tokyo Commodity Exchange (TOCOM), so other terms should be read accordingly.

Reference: The method for calculating the amount of margin requirement was changed from the one based on SPAN[®] (Note: SPAN[®] is a margin calculation method developed by the Chicago Mercantile Exchange) to the VaR (Value at Risk) method in November 2023.

(3) Key Management Checkpoints

- i. Regarding margin management, are internal rules (internal regulations or operating rules) and administrative processes (including management of agreements for setting up trading accounts and security deposit receipts related to commodity futures and options) being properly implemented?
- ii. Are allocations or positions properly reported (close-out report or position by customer report)?
- iii. Have open position limits been properly established for customers, and is

compliance with these limits being properly checked?

- iv. When a customer's futures or options transaction is executed, is the margin for the transaction received appropriately? When an insufficient amount of margin has been or is likely to be received from a customer, is the customer managed appropriately? Please note that when a customer uses cross margining²², the effect of the cross margining must be considered when calculating the customer's margin requirements. In addition, when a commodity futures transaction is settled by delivery, delivery clearing margin²³ must be deposited.
- v. When the firm receives from a customer an amount of margin that exceeds the required amount, does it deposit the full amount with JSCC? (Does it ensure that a situation does not occur in which only the required amount is deposited by mistake?)
- vi. When a trading participant (clearing participant) uses its own funds to deposit a customer's add-on initial margin (based on risk amount or based on stress loss over IM (SLOIM)) with JSCC, has the participant obtained the customer's agreement to do so? In addition, has the participant submitted an application to JSCC to do so?
- vii. When an emergency margin call or other margin call is made, does the firm's operational system function appropriately? Does it enable a swift internal response?
- viii. Are internal inspections and examinations performed to determine the management status of margins for futures and options trading? If they are, what do they focus on and with what frequency are they being performed?

²² Cross margining enables the offsetting of risks related to JGB futures transactions, interest rate swap (IRS) transactions, and interest rate futures transactions. Its purpose is to reduce the collateral burden on JSCC's clearing participants for such transactions.

²³ Delivery clearing margin refers to the amount of margin that is required when a commodity futures transaction is settled by delivery and is the amount that is calculated based on Appendix 3 "Table Concerning Calculation of Required Amount of Delivery Clearing Margin" of JSCC Rules on Margins, etc. for Futures and Options Contracts.

14. Credit Management for Margin Trading, etc.

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 56-2.1
- Supervision Guidelines: IV-2-4 Counterparty Risk Management Framework, others

Reference: Overview of Securities Firm Examination Results for OHT Inc. issued by the Securities and Exchange Surveillance Commission on February 8, 2008

(2) Regulatory Intent and Requirements

There is a broad range of risks inherent to the operations of financial instruments business operators, and accurately identifying and properly managing them is critical for the protection of investors and, by extension, stability of the financial system. JPX-R inspections of risk management systems, therefore, are performed with attention focused on particular types of risk and are based on considerations of both the Supervision Guidelines and the connection between firms and exchange trading. Regarding systems for managing credit risks related to margin trading, in particular, JPX-R, given TSE's past experience in this area, requests trading participants to perform internal inspections and, in its own inspections, examines how each company addresses and manages these risks.

More specifically, JPX-R looks at the types of customers handled by each trading participant, and examines whether management of customer margin maintenance rate, credit limit management, and after-the-fact handling of additional margin and advances are being properly addressed in light of risk management and other considerations.

(3) Key Management Checkpoints

- i. From the perspectives of factors like customer financial wherewithal and investment experience, have appropriate standards been established for opening accounts of margin trading (including when-issued transactions; the same hereinafter) and trading of options on futures? Are inspections performed based on these standards? If when-issued transactions are handled, are they being handled with the same approaches used for margin trading (same applies below)?
- ii. Have internal rules for establishing account-opening standards and conducting inspections of account-opening operations been provided?
In addition, is the enforcement status of these rules being properly checked with appropriate timing?
- iii. Have open position limits and other credit limits been established for individual customers? In addition, are an alarm system and other measures used to properly monitor the activities of customers who trade stocks, etc. on margin or options on futures?

- iv. Have internal rules for enhancing position limits (per customer or issue) standards been provided? In addition, when enhancing position limits of certain customers, are proper checks made in terms of counterparty risk?
- v. Does the firm use a designated unit and designated personnel to monitor the direction of margin transactions or options on futures trading? In addition, how does the firm determine whether it has customers that are unusual in terms of outstanding margin transactions or margin trading conditions, and how does it monitor their activities in particular?
- vi. Are proper measures or responses taken to customers whose trading balance or activities are considered to be unnatural, such as imposition of a ban on new positions?
- vii. When an issue is designated as "issues subject to daily disclosure" or "issues under observance", or other regulatory actions pertaining to margin trading are taken, is that information properly communicated within the firm, and are relevant personnel properly informed?
- viii. With regard to issues subject to daily disclosure and issues under observance, how does the firm determine whether it has customers who are engaged in related trading or have unusual activity, and how does it continuously follow up on their activities?
- ix. For issues under observance, in particular, are transaction and customer management being properly performed in light of liquidity risk and other factors?
- x. Are proper measures established against the practice of nikai-date margin positions in which securities purchased on margin are used as collateral for further margin purchases?
- xi. Have customer margin maintenance rate, collateral/deposit check, and other alarm points been established to prevent the development of advances for margin transactions or trading of options on futures?
- xii. Have measures been taken to prevent the expansion of advances for margin transactions or options on futures trading? Is additional open interest not permitted, when the maintenance ratio is still below requirements?
- xiii. In terms of credit management, how does firm handle cases where the self-regulatory organization has made inquiries about a specific customer? (For example, are internal examinations of matters, such as customer backgrounds and trading motives, immediately performed?)
- xiv. What kinds of management measures have been taken with regard to customers in internet, call center, and other types of non-in-person transactions, which involve risks different from those associated with in-person transactions?

- xv. Regarding the status of credit management (including management measures addressed above) for margin transaction or options on futures trading, how are inspections (scheduled and unscheduled) of risk management effectiveness checked?

15. Internal Audit System

(1) Relevant Laws, Rules, and Regulations

- FIEA: Article 56-2.1
- Supervision Guidelines: III-1-(1)-(iv) Internal Audit Section, others

Reference: Matters concerning internal audit systems are included among the items inspected for application for the registration of Type I Financial Instruments Business.

(2) Purpose of Inspections

According to the Supervision Guidelines, "internal audits are conducted by entities independent from audited divisions, in order to examine and evaluate the status of business execution and the appropriateness, effectiveness and reasonableness of internal management and control, and to provide advice and make recommendations to the management based thereon, with a view to contributing to the achievement of the management goals of Financial Instruments Business Operators."

In addition, the internal audit function is expected to: 1) examine and evaluate the appropriateness and effectiveness of operational execution and internal management; 2) make recommendations to management on how to rectify management deficiencies identified; and 3) act, via examinations and recommendations for improvements from an independent position, as an internal check on audited divisions. Given the importance of internal audit functions, JPX-R inspections examine the condition of the internal audit system in companies subject to inspection and seek to determine whether they are being performed effectively while focusing on matters like conditions with regard to internal rules and the firm's organization related to internal audits, status with regard to the performance of internal audits, and the rectification of deficiencies.

On the other hand, even if there is no dedicated internal audit division, inspections and confirmation focus on how the internal audit functions are being carried out. These include 1) examining and evaluating the appropriateness and effectiveness of operational execution and internal management; 2) making recommendations to management on how to effect improvements; and 3) acting as an internal management on audited divisions.

(3) Key Regulatory Checkpoints

- i. In addition to the rules forming the basis of internal audits, have detailed rules and manuals been prepared? If they have, what are the purposes and what do they require?
- ii. Do internal rules provide that the division in charge of internal audits (hereinafter "internal audit division") is to audit not only sales divisions but also internal management divisions and all other divisions? Furthermore, has the internal audit division been given the authority to obtain all information required for it to perform its duties and the authority to interview and ask questions of all executives and employees?

- iii. What is the status of the internal audit division's organization? If the internal audit division is actually comprised of multiple units, what duties are performed by each of the units, and what is the status of conditions with regard to a communication system linking all of the units?
- iv. Has the internal audit division secured enough independence from sales divisions and other audited divisions to sufficiently perform its internal management function? In addition, if independence is lacking, what steps are being taken to ensure the effectiveness of internal audits?
- v. Does management sufficiently recognize the importance of the role performed by the internal audit division, and has it assigned to the internal audit division personnel in appropriate numbers and with appropriate backgrounds to provide it with knowledge of operations of each audited division and ensure it is capable of performing its role?
- vi. What are the key drivers underlying annual internal audit planning by the internal audit division? For example, are the basic elements of internal audit plans—the direction to be taken with audits, audit schedule, and key audit concerns—determined based on the types and degrees of risks and on the status of internal management in audited divisions?
- vii. Do internal audit plans receive prior approval by not only the head of the internal audit division but also the firm's management? Also, does management direct the head of the internal audit division to change the internal audit plans when warranted by the emergence of a significant management problem or changes in the business environment?
- viii. What is the workflow used for internal audits? In particular, if internal management problems or illegal activity are identified through an internal audit, what specific actions are taken in response?
- ix. If part of the operations of an audited division has been delegated to another unit, is the management of that other unit subjected to internal audit procedures?
- x. Do conditions permit the internal audit division to swiftly gain access to the results of internal inspections performed by audited divisions? In addition, what does the internal audit division do with these results when it performs an internal audit?
- xi. Do audited divisions reliably implement improvements based on internal audit findings? Furthermore, does the internal audit division properly determine whether audited divisions have made improvements in response to audit findings, and how does the internal audit division reflect improvements or the failure to make improvements in future internal audit plans?
- xii. If the firm is subject to inspections, does it, in addition to performing internal audits, also make use of external audits (as mainly operational audits) tailored to

the unique characteristics of its operations? Or, is it considering doing so?

- xiii. Are the key findings of external audits reported to management and the Board of Statutory Auditors without delay? In addition, do audited divisions make improvements in response to external audit findings within a certain timeframe, and does the internal audit division properly identify and examine these improvements?
- xiv. Does the internal audit division have policies, such as ones for improving the expertise of auditors by having them participate regularly in internal and external training that is aimed at improving internal audit functions?

16. Exchange System Connection Management

(1) Relevant Laws, Rules, and Regulations

- TSE Business Regulations: Rule 77.2
- TSE Brokerage Agreement Standards: Rules 8 and 9
- OSE Business Regulations: Rule 51.2
- OSE Brokerage Agreement Standards: Rules 11 and 11-2
- TSE/OSE/JPX-R Order Management Guidelines
- Items to observe when making a connection to the respective systems of TSE and OSE, their interface requirements or specifications, etc.

(2) Purpose of Inspections

As mentioned in 11. Measures to Prevent Erroneous Orders, due to recent technological advances and low latency trading, trading based on automated order placement by using an electronic data processing system continues to expand.

In conjunction with this, there is an increasing risk of unexpected and erroneous order placement (the placement of many small sliced orders that result in an excessively large combined quantity or monetary amount) due to malfunction in electronic data processing systems, which may have a significant impact on the market. Therefore, in order to prevent such erroneous order placement, trading participants are required to implement appropriate restrictions on orders.

The same can be said for all inter-system communications between trading participants and exchanges, not necessarily limited to order placement. In other words, as trading participants and investors such as low latency traders have improved the performance of their electronic data processing systems in response to the recent increase in trading speed, the risk of malfunctions causing a significant volume of abnormal communications and overloading the systems of exchanges receiving such communications is increasing. In an extreme case, it could even bring down exchange trading systems, which would have a tremendous impact on the market. Therefore, trading participants are required to set system-based restrictions to prevent the occurrence of a large volume of irregular transmissions and establish monitoring systems to detect them, as well as those that enable a prompt response to their occurrence.

Meanwhile, TSE and OSE have been working to enhance their ability to respond to and recover from unexpected events (i.e., their resilience). As part of these efforts, they have clarified that in the event of a failure in the exchanges' trading systems, trading may resume after the accepted orders have been cancelled. Trading participants are required to determine ahead of time how orders will be handled after trading has resumed and to take the necessary actions on their customers' behalf. In its inspections, JPX-R confirms the status of a trading participant's compliance with such requirements while also paying attention to the coordination among the trading participant's compliance, systems, and other divisions as well as the trading participant's cooperative relationships with system vendors and other outsourcees.

(3) Key Regulatory Checkpoints

- i. Has the trading participant implemented appropriate management to prevent transmissions that would cause excessive burden to the exchange trading systems or that are not related to business?
- ii. For messages such as those related to business and TCP/IP, have the restriction on the number of retries and intervals for retries been set in the event of errors in login or connection establishment?
- iii. How is the monitoring of irregular transmissions being conducted? Have system settings and management structures been in place to immediately shut down the connection to the exchanges if irregular transmissions are recognized, or a notification from an exchange of an unauthorized transmission is received?
- iv. Has the handling of unexecuted orders (those on the exchange's order book) in the event of a disconnection been considered in advance?
- v. Are the settings of a server number, user ID, IP address, port number, or any other information used for inter-system connections to exchanges properly checked and controlled, rather than leaving them completely up to the system vendor?
- vi. Are there multiple communication paths that can be switched to counter failures and any other errors of an exchange trading system server?
- vii. Has the trading participant already determined how to respond to cases where a failure occurs in an exchange trading system and trading resumes after unexecuted orders (those on the order book) are cancelled? If the participant has determined that they will not resend such orders, has it informed the customer of the fact in advance?
- viii. Has the trading participant determined whether or not it participates in trading after trading resumption to be able to respond to the exchange about the participation? Has the trading participant participated in drills for such response?
- ix. If a customer has a system with software managed by the customer, does the trading participant check and provide guidance, among others, to the customer, while giving sufficient consideration to its cyber security management and IT systems risk management such as development as well as operation and management of the system? For example, can the trading participant check the status of IT systems risk management such as cyber security management by sending questionnaires to customers or any other means, conduct risk assessment, establish a system to identify changes, or others in the management status, and encourage customers to take actions as necessary?
- x. If a customer has a system with software managed by the customer, what is its status with respect to checkpoints i. through iv. above?

- xi. Has a trading participant placed orders or transmitted other data for testing purposes without "actual demand" during production operation of the exchange trading systems?

17. Miscellaneous (1-2)

1. Regarding the submission of the Report on Activities Violating Laws, Regulations, and Rules and the Report on Computer System Malfunctions

In May 2007, TSE and OSE implemented revisions to its Trading Participant Regulations and some of its other rules, changing provisions regarding the reports trading participants submit to TSE or OSE. Among these changes are requirements to submit two new reports: the Report on Activities Violating Laws, Regulations, and Rules (hereinafter the "Regulatory Violation Report") and the Report on Computer System Malfunctions (hereinafter the "Computer System Malfunction Report"). TSE is requiring the submission of these reports, so that it can have clear information on the status of regulatory violations and system malfunctions among trading participants.

Regulatory Violation Reports incorporate two key aspects. One is offsite monitoring of regulatory violations at individual trading participants. The other is the ability to confirm each trading participant's ability to clean up its own operations. Regarding the latter, in particular, the discovery of illegal activities by trading participants themselves, through internal inspections, and other developments showing the effectiveness of trading participant's self-discipline and governance to sustain compliance have demonstrated that Regulatory Violation Reports have also been useful for confirming the status of internal management at the trading participants that submit them.

The Computer System Malfunction Report, on the other hand, gives TSE and OSE a better picture of the status of malfunctions in trading participant computer systems and allows it to respond more swiftly in analyzing the causes of problems and identifying IT systems risks impacting TSE or OSE.

Both reports must be submitted to TSE or OSE (TSE/OSE Market Participants Relations Office) together with notifications and reports submitted to regulatory authorities when violations or malfunctions occur. Reports on violations of TSE/OSE regulations may be submitted on a monthly basis.

Reference Notice:

- TSE Notice regarding the submission of "Report on Activities Violating Laws, Regulations, and Rules", etc. (dated May 25, 2007)
- TSE Notice regarding the revision of "Appendix: Items to be Submitted Regarding Violation of Rules and Regulations" (dated July 3, 2020)

2 . Regarding internal inspection requests from JPX-R's Trading Participants Examination & Inspection Department

Based on violations discovered in past inspections, JPX-R's Trading Participants Examination & Inspection Department asks trading participants to perform internal inspections as a preventive measure and encourages them to voluntarily comply with its requests. These requests, which began in fiscal year 2005, are made in regard to the following items.

| Request Date | Inspection Items | |
|------------------------|--|--|
| April 2005 | Same-day cash collection regulations | Inspection to determine the status of efforts to inform personnel on the details of regulatory measures and the status of efforts to prevent evasion of these regulations |
| April 2005 | Front running prevention management | Inspection of firewall measures taken to separate units executing customer orders from units executing orders for the firm's own account |
| April 2005, April 2007 | Margin trading deposit calculation (1, 2) | Inspection to determine whether there have been any offsets of undelivered settlement losses against settlement gains, and inspection regarding the calculation methods used for actual-receipt/actual-delivery transactions and other matters |
| May 2006 | Best execution duty | Inspection of the status of efforts to prevent the receipt of orders without prior provision of best execution policies in written form and other matters |
| May 2006, April 2007 | Measures to prevent erroneous order placement (1, 2) | Inspections to determine the status of limit settings on all order terminals for all products, the appropriateness of limit levels, and other matters |
| April 2007 | Net settlement transactions | Inspection of the management methods used to secure purchase money from internet transaction customers |
| April 2008 | Credit risk management | Inspection of specific management checkpoints for credit risk related to margin trading (in light of the OHT, Inc. incident) |
| May 2009 | Stabilization trading regulations (Reporting obligation) | Inspection of measures to provide customers with information on all communications from TSE on stabilization trading |
| June 2010 | Measures to prevent erroneous order placement (3) | Inspection to determine the status of limit management measures following the startup of TSE's arrowhead and Tdex+ systems, inspection to ensure terminals with low usage frequencies have not been overlooked in setting limits, and other matters |
| February 2012 | Dummy order placement and other acts during live operation hours of exchange trading systems | Inspection of whether or not there is any order placement or other data transmission that is not in accordance with actual demand for test purposes such as specification or operational checks was carried out during live operation hours of TSE trading systems |

| Request Date | Inspection Items | |
|---------------|--|--|
| June 2013 | Trading limits to prevent erroneous orders | Inspection of trading limits following the cash market integration between TSE and OSE |
| December 2013 | Trading limits to prevent erroneous orders | Inspection of trading limits following the derivatives market integration between TSE and OSE |
| March 2015 | Trading limits to prevent erroneous order placement | Inspection of trading limits following the renewal of arrowhead |
| February 2016 | Management of Corporate Information | Inspection of whether there is an appropriate management system to thoroughly check whether information acquired by an analyst or other company employee is corporate information and to prevent solicitation using corporate information |
| June 2018 | Data Linkage with Trade Surveillance System | Inspection of whether information pertaining to transactions (own-account and customer-account) that were handled by the trading participant was incorporated appropriately into the trade surveillance system and whether there were no transactions that were missing from searches for transactions subject to trade surveillance |
| June 2025 | Trading Supervision Response Following the Introduction of the Closing Auction Session | Inspection of whether the measures taken in response to the revision of the guidelines (i.e., revision of internal rules and manuals pertaining to trade surveillance, changes to the parameter settings in the trade surveillance system) had been completed |

Revision History

| | |
|--------------------|--------------|
| March 24, 2009: | 1st Edition |
| February 10, 2010: | 2nd Edition |
| March 8, 2011: | 3rd Edition |
| February 29, 2012: | 4th Edition |
| March 4, 2013: | 5th Edition |
| March 5, 2014: | 6th Edition |
| January 6, 2015: | 7th Edition |
| February 28, 2017: | 8th Edition |
| June 27, 2018: | 9th Edition |
| June 26, 2020: | 10th Edition |
| August 12, 2021: | 11th Edition |
| October 7, 2022: | 12th Edition |
| May 7, 2024: | 13th Edition |
| January 21, 2026: | 14th Edition |

DISCLAIMER: These materials were prepared for informational purposes only. Reproduction or distribution by any means for commercial purposes is prohibited. While every effort is taken to ensure the accuracy of the information contained in these materials, JPX-R bears no responsibility or liability for any actions that may be taken based on these materials.

This translation may be used for reference purposes only. This English version is not an official translation of the original Japanese document. In cases where any differences occur between the English version and the original Japanese version, the Japanese version shall prevail. This translation is subject to change without notice. Japan Exchange Group, Inc., and/or its affiliates shall individually or jointly accept no responsibility or liability for damage or loss caused by any error, inaccuracy, misunderstanding, or changes with regard to this translation.

Copyright © 2009-2026 Japan Exchange Regulation, All rights reserved.