(Comprehensive Supervision Guidelines for Financial Instruments Firms, etc. (Comparison Table of Old and New Provisions) (Draft)

Revised Draft	Current
III. Supervisory Evaluation Items and Procedures (General Provisions)	III. Supervisory Evaluation Items and Procedures (General Provisions)
III-2-8 System Risk	III-2-8 System Risk Management Framework
III-2-8-1 System Risk Management Framework	(New)
(1) Key Focus Areas	(1) Key points
①–④ (omitted)	①～④ (omitted)
⑤ Cybersecurity Management	⑤ Cybersecurity Management
(i) The Board of Directors and other relevant bodies recognize the importance of cybersecurity and and have established necessary measures in accordance with the "Guidelines on Cybersecurity in the Financial Sector."	(i) The board of directors and other relevant bodies recognize the importance of cybersecurity and and have established necessary measures in accordance with the "Guidelines on Cybersecurity in the Financial Sector."
(ii) When conducting non-face-to-face transactions using communication means such as the Internet (hereinafter referred to as "Internet transactions"), –2–8–2–2.	(ii) When conducting non-face-to-face transactions using communication means such as the internet, have appropriate authentication methods commensurate with the risks of such transactions been introduced? ■ Authentication methods that do not rely solely on fixed IDs and passwords, such as variable passwords or electronic certificates ■ Transaction authentication using multiple paths, such as using a mobile phone or other device separate from the browser of the computer used for the transaction ■ Transaction authentication using hardware tokens or similar methods for transaction signatures (Note) Measures to prevent unauthorized withdrawals from customer accounts due to unauthorized access (e.g., procedures for designating or changing the destination financial institution account (withdrawal destination account) , the customer

amendment proposal	Current
⑥～④ (omitted) (2)(3)(omitted)	We do not permit the designation or change of a withdrawal destination account with a different account name, and we take measures to prevent transfers to withdrawal destination accounts with different account names by, for example, sending written documents for account designation or change procedures to the customer's address via registered mail. In such cases, it is considered that appropriate measures commensurate with the risks of the transaction have been taken. (c) When conducting non-face-to-face transactions using communication means such as the internet, are appropriate measures to prevent fraud implemented in accordance with the nature of the business, such as the following? ■ Providing users with security software capable of detecting and removing viruses during transactions ■ Implementation of software that detects virus infections on customers' computers and issues warnings to the financial instrument firm ■ Adoption of a method where electronic certificates are stored on a separate medium or device from the computer used for transactions, such as an IC card ■ Establishing a system to promptly notify users of unauthorized logins or abnormal transactions, etc. (Reference) ■ Guidelines for Preventing Unauthorized Access in Internet Transactions (July 20, 2021: Japan Securities Dealers Association) ■ Guidelines for Preventing Unauthorized Access in Internet Transactions (August 18, 2021: Financial Futures Association of Japan) ⑥～④ (omitted) (2)(3)(omitted)

Amendment Proposal	Current
III-2-8-2 Internet transactions	(Newly added)
III-2-8-2-1 Significance	(Newly added)
Internet transactions enable financial instrument firms to provide services at low cost and offer users a convenient transaction tool. However, since internet transactions are conducted non-face-to-face, they entail unique risks such as the inability to detect abnormal transaction patterns. When providing services to customers, financial instruments firms are required to safely manage customers' assets. Therefore, from the perspective of ensuring customer convenience while thoroughly protecting customers, it is important for financial instruments firms to implement adequate security measures related to internet trading, as well as to provide information, education, and promote awareness among customers.	
III-2-8-2-2 Key Points (1) Establishment of Internal Management Systems In light of the increasing sophistication and complexity of criminal activities such as unauthorized access and unauthorized transactions via the internet, and the resulting expansion of damages, this should be positioned as one of the top management priorities. The board of directors or equivalent body should conduct necessary reviews and strive to enhance security levels. and provide customers with necessary precautions and other information when using the system.	(New)

Revised Proposal	Current
Is the necessary infrastructure in place to provide explanations? Additionally, to ensure the sound and appropriate operation of internet trading, is there a system in place within the financial instruments business operator to ensure that all departments share an accurate understanding of the situation and work together as an organization? In doing so, are they utilizing information-sharing organizations such as the Financial ISAC or JPCERT/CC to provide and collect information on the occurrence of crimes and criminal methods, share effective countermeasures, and conduct discussions tailored to the characteristics of their own customers and operations? Are they also considering measures to address criminal methods that may arise in the future and striving to establish necessary systems? Additionally, is the so-called PDCA cycle—comprising risk analysis, the formulation and implementation of security measures, verification of their effectiveness, and the evaluation and review of measures—functioning effectively? (2) Ensuring Security Are measures being taken in accordance with the characteristics of their customers and business operations, based on an understanding of the risks at each stage of security system development and use? Are multiple effective measures being combined to improve overall security, rather than taking ad hoc measures, and are the necessity and type of measures being determined based on a thorough understanding and assessment of risks, with rapid response measures in place? Are policies on information security in general related to Internet transactions being formulated, and are the effectiveness of such policies against various crime methods being verified, with necessary revisions being made as necessary? . Are you also establishing a system to review these policies as necessary in accordance with the relevant guidelines? Are you implementing measures in accordance with these policies?	

Amendment Proposal	current
,taking into account the attributes of individual and corporate customers,andin accordance with the"Guidelines on Cybersecurity in the Financial Sector" and the Japan Securities Dealers Association's "Guidelines for Preventing Unauthorized Access, etc. in Internet Transactions," and other relevant guidelines, and are appropriate security measures being implemented in accordance with the content of the services provided? In doing so, are considerations being given to the sophistication and ingenuity of criminal methods (such as "man-in-the-middle attacks" and "man-in-the-browser attacks")? Additionally, regarding countermeasures against phishing fraud, are appropriate measures being taken to prevent users from being prompted to enter passwords on pages or links within emails or SMS (short message services) (excluding cases where alternative measures are not feasible due to legal obligations) to confirm that the site accessed by users is authentic, to implement domain authentication technology in a planned manner, and taking appropriate countermeasures against phishing, such as requesting the closure of phishing sites, depending on the content of the services provided. (Note) When collecting information, it is advisable to utilize information on criminal methods provided by financial institutions, financial information system centers, the Financial Services Agency, and police authorities. When conducting internet transactions, are appropriate measures to prevent fraud implemented in accordance with the content of the services provided? Additionally, are risks regularly and timely recognized and evaluated in light of changes in domestic and international environments and the occurrence of accidents or incidents, and are authentication methods, etc., reviewed as necessary?	

Amendment Proposal	Current
■ Implementation and mandatory use (set as default) of phishing-resistant multi-factor authentication (e.g., authentication using passkeys, authentication based on PKI (public key infrastructure)) for important operations such as login, withdrawal, and changing the withdrawal destination bank account. (Note 1) After implementing and making multi-factor authentication resistant to phishing mandatory, if customers are unable to set up multi-factor authentication due to reasons such as not owning the necessary devices (e.g., smartphones), alternative multi-factor authentication must be provided. Additionally, the implementation must monitor the rate of such exemptions, consider advancements in authentication technology and standards, and review and implement improvements to the multi-factor authentication methods to reduce the exemption rate. (Note 2) Until phishing-resistant multi-factor authentication is implemented and made mandatory, alternative multi-factor authentication must be provided, and customers must be notified of the specific schedule for implementation and mandatory use. In addition, detection functions such as behavior detection and login notifications must be strengthened during this period. ■ Provide a function to notify customers via email or other means to detect unauthorized logins, transactions, withdrawals, or changes to withdrawal destination accounts by unauthorized third parties. ■ Implement and require an automatic account lockout feature that stops login attempts after consecutive failed authentication attempts. ■ Implementation of behavior analysis during customer login to detect unauthorized access (Behavior detection during login) and implementation of the retention of login and transaction information for post-incident verification ■ Implementation of additional identity verification based on the evaluation of unauthorized access	

Revised proposal	Current
or timely blocking of access suspected of unauthorized access, blocking access from the source of unauthorized access, and other appropriate measures ■ Other measures specified as "Standards" (measures that must be implemented reliably) in the Japan Securities Dealers Association's "Guidelines for Preventing Unauthorized Access in Internet Transactions" Furthermore, are the following unauthorized access prevention measures in place? ■ Providing multi-factor authentication resistant to phishing during transactions or when providing services linked to other bank accounts ■ Providing customers with the ability to set transaction amount limits and the scope of purchasable products ■ Establishing a system to detect unauthorized logins or abnormal transactions and promptly notify users ■ Implementation of measures designated as best practices (recommended for implementation) in the Japan Securities Dealers Association's "Guidelines for Preventing Unauthorized Access and Other Unlawful Acts in Internet Transactions" (Reference) ■ Guidelines for Preventing Unauthorized Access in Internet Transactions (Japan Securities Dealers Association) ■ Guidelines for Preventing Unauthorized Access in Internet Trading (Financial Futures Association of Japan) ■ Security Standards and Guidelines for Computer Systems of Financial Institutions (Financial Services Agency)	

Revised Draft	Current
Financial Information Systems Center) ■ Phishing Countermeasure Guidelines (Phishing Countermeasure Council) (3) Customer Support Is there a system in place to adequately inform customers about various risks, such as the danger of theft of personal information such as IDs and passwords on the Internet, the danger of using easily guessed passwords (limited to cases where passwords are used for authentication) and the possibility of damage spreading, as well as to raise awareness through examples of security measures required of customers? Are measures in place to enable customers to promptly recognize any damage they have suffered? Is a system in place to promptly receive reports from customers? In addition, is a system in place to promptly notify customers (including public disclosure) in a manner that is easy for them to understand when necessary? In particular, if it is possible to identify customers who may be affected, are measures in place to minimize damage by contacting them as quickly as possible? Are measures in place to regularly monitor the adoption of countermeasures to prevent unauthorized transactions among users, and are additional measures being implemented to promote their adoption? In the event of damage caused by unauthorized transactions, are measures in place to thoroughly investigate the extent of the damage, taking into account the circumstances of the customer and other relevant factors, and to provide compensation to the customer and other measures to restore losses, and is the necessary infrastructure in place to conduct sincere customer service in such cases?	

Amendment Proposal	current
? Are records related to unauthorized transactions appropriately retained, and when requested by customers or investigative authorities to provide such materials, is there a commitment to cooperate sincerely? (4) Other Are measures in place to establish customer management systems, including customer verification procedures, taking into account the nature of internet transactions as non-face-to-face transactions? If outsourcing is utilized for internet transactions, have the risks associated with such outsourcing been assessed, and have necessary security measures been implemented? III-2-8-2-3 Supervision Methods and Responses (1) In the event of a crime Upon detecting unauthorized access or unauthorized transactions in internet transactions, promptly request the submission of a "Crime Occurrence Report" to the relevant authorities. Note that the Financial Bureau shall immediately notify the relevant department of the Financial Services Agency upon receiving a report from a financial instruments business operator. (2) When issues are identified If, based on inspection results, the Crime Report, or other relevant information, there is reasonable suspicion that the financial instruments business operator is not conducting its internet-related business operations in a sound and appropriate manner, additional measures shall be taken as necessary in accordance with Article 56-2, Paragraph 1 of the Act.	(newly established)

amendment proposal	current
report. If, after such review, necessary measures such as crime prevention strategies or responses following the occurrence of damage are not implemented, and situations such as the recurrence of damage arise, or if it is deemed necessary from the perspective of investor protection, measures such as issuing a business improvement order pursuant to Article 51 of the Act shall be taken. III-3 Procedures (General Provisions) III-3-3 Records and Documents Related to Business Operations (1) Basic Considerations ① to ⑧ (omitted) ⑨ The latter part of the proviso of Article 157, Paragraph 3, and the proviso of Article 181, Paragraph 4, of the Ordinance on Commercial Affairs, etc., shall apply regardless of whether the books and documents listed in the items of Paragraph 1 of the same article were created at a business office or office established abroad, provided that such books and documents are created in electronic form and are kept in a state where the information recorded in such electronic records can be promptly viewed at a business office or branch established within Japan, such books and documents may be preserved abroad. However, financial instrument firms must give sufficient consideration to information management systems (III-2-4) and system risks (III-2-8) related to customer information, and must also appropriately consider the risk of unauthorized access, information leakage to third parties, or disruptions to system stability in the foreign country where the records are stored. must also be appropriately considered.	III-3 Procedures (General Provisions) III-3-3 Records and Documents Related to Business Operations (1) Basic Considerations ①–⑧ (omitted) ⑨ The provisions of the latter part of Article 157, Paragraph 3, and Article 181, Paragraph 4, of the Commercial Code, as amended, shall apply regardless of whether the books and records listed in the items of Paragraph 1 of the same article were created at a business office or branch established abroad, provided that such records are created in electronic form and that the information contained therein is promptly made available for inspection at a business office or branch established within Japan. However, financial instrument firms must ensure that they have adequate measures in place for managing customer information (III-2-4) and system risk management (III-2-8), and must also appropriately consider the risk of unauthorized access, information leakage to third parties, or disruptions to system stability .

Amendment Proposal	Current
IV. Supervisory Evaluation Items and Procedures (Investment Management Business)	IV. Supervisory Evaluation Items and Procedures (Investment Management Business)
IV-3-7 Appropriateness of Business Operations of Financial Instruments Firms Handling Rights to Electronic Record Transferable Securities	IV-3-7 Appropriateness of Business Operations of Financial Instruments Firms Handling Electronic Record Transfer Securities and Related Rights
IV-3-7-5 System Risk Management Framework	IV-3-7-5 System Risk Management Framework
In conducting transactions such as the purchase and sale of electronic record transferable securities and related rights, the nature of such business often requires the use of highly sophisticated and complex information systems that rely on the internet. Additionally, electronic record transferable securities and related rights represent property value recorded electronically on platforms such as blockchain and transferable via networks. As a result, the risk of unauthorized access or leakage of important information due to cyberattacks, which are becoming increasingly sophisticated, has grown significantly. Additionally, financial instrument firms may outsource these operations to third parties or use a common network jointly designed and developed by multiple financial instrument firms. In such cases, in addition to the points outlined in Sections III-2-8-1(1) and III-2-8-2-2, verification should be conducted on the following points, for example:	In the trading or other transactions involving electronic record transferable securities, the nature of such business often requires the use of highly sophisticated and complex information systems based on the internet. Additionally, electronic record transferable securities represent property value recorded electronically on blockchain or similar technologies and transferable via networks. As a result, the risk of unauthorized access or leakage of important information due to cyberattacks, which are becoming increasingly sophisticated, has grown significantly. Additionally, financial instrument firms may outsource these operations to third parties or use a common network designed and developed jointly by multiple financial instrument firms. In such cases, in addition to the points outlined in Section III-2-8(1), verification should be conducted on the following points, for example:
(1) to (5) (omitted)	(1) to (5) (omitted)
IV-3-7-6 Matters to be noted regarding segregation of assets	IV-3-7-6 Matters to be noted regarding segregation of management

Amendment Proposal	Current
(1) (omitted) (2) When a financial instruments business operator entrusts the management of rights to electronic record transfer securities to a third party ① (omitted) ② The financial instruments business operator, as the entrusting party, must ensure that the entrusted party manages the rights and interests in electronic records in accordance with the provisions of Section III-2-8-1(1)(viii) and IV-3-7-5(4) of the aforementioned III-2-8. VIII. Supervisory Evaluation Items and Procedures (Registered Financial Institutions) VIII-1 Appropriateness of Operations (Registered Financial Institutions) The appropriateness of the business operations of registered financial institutions shall be evaluated in accordance with the provisions of Section III-2 (Section III-2-3-2-4 (3), III-2-6(1)③ and ⑤, III-2-8-1(3), III-2-9, and III-2-15), IV-1-3, IV-3-1(IV-3-1-2 (1), IV-3-1-4 (6), and IV-3-1-5 excluded), IV-3-2-3(4), IV-3-3 (IV-3-3-1 (1)(2), and (4), IV-3-3-2 (4)③ to ⑧, IV-3-3-4 (1) and (2) and IV-3-3-5 are excluded. However, this does not apply if the registered financial institution engages in foreign exchange margin trading as a business.) IV-3-5 (excluding IV-3-5-4), IV-3-7, V-2-4 (excluding V-2-4-4), V-2-5, VI-2 (excluding VI-2-2-1 (1) (vii) to (ix) and VI-	(1) (omitted) (2) When a financial instruments business operator entrusts the management of electronic record transferable securities representation rights, etc., to a third party ① (omitted) ② The financial instruments business operator, as the entrusting party, shall ensure that the entrusted party manages the rights to electronic record transfer securities in accordance with the provisions of Section III-2-8 (1) (viii) and IV-3-7-5 (4) of the aforementioned III-2-8. VIII. Supervisory Evaluation Items and Procedures (Registered Financial Institutions) VIII-1 Appropriateness of Operations (Registered Financial Institutions) The appropriateness of the business operations of registered financial institutions is evaluated in accordance with the provisions of Section III-2 (Section III-2-3-2-4 (3), III-2-6 (1)③ and ⑤, III-2-8 (3), III-2-9, and III-2-15), IV-1-3, IV-3-1(excluding IV-3-1-2(1), IV-3-1-4 (6), and IV-3-1-5), IV-3-2-3(4), IV-3-3 (IV-3-3-1 (1)(2), and (4), IV-3-3-2 (4)③ to ⑧, IV-3-3-4 (1) and (2), and IV-3-3-5, However, this does not apply if the registered financial institution engages in foreign exchange margin trading as a business.), IV-3-5 (excluding IV-3-5-4), IV-3-7, V-2-4 (excluding V-2-4-4), V-2-5, VI-2 (excluding VI-2-2-1 (1) (vii) to (ix) and VI-

Amendment Proposal	Current
2-2-5 (excluding (2) and (3)) and VII-2, and shall also take into account the following points: Note that regarding financial product intermediary services, the theoretical prices under IV-3-1-2(6)(iii)(i) and (ii), as well as the internal rules under (iii)(ii) and (iv), may be used as those calculated or established by the commissioned financial product trading company. may be used.	2-2-5 (2) (3) are excluded) and VII-2, and the following points shall be noted. Note that for financial product intermediary services, the theoretical prices specified in Section IV-3-1-2(6)(iii)(i) and (ii), as well as the internal rules specified in Section IV-3-1-2(6)(iii)(ii) and (iv), may be used if they are calculated or established by the commissioned financial product trading company. may be used.