

Main Topics Raised by the Financial Services Agency (FSA) at a Dialogue Meeting with the Industry Association

[Held on June 16, 2026 (with the Japan Securities Dealers Association (JSDA))]

1. International Organization of Securities Commissions (IOSCO) Annual Meeting

- The IOSCO Annual Meeting was held from May 11 to 14, 2026. It was originally scheduled to be held in person in Sharm El-Sheikh, Egypt, but was changed to an online format in light of the situation in the Middle East. In addition to the Presidents Committee meetings, various meetings such as the Board meetings and the Regional Committee meetings were held, and a wide range of issues were discussed. The Board discussed market developments, the risk outlook, financial stability, and risks and opportunities posed by new technologies such as AI and digital finance. The Board also approved the publication of several reports. Among these, we will highlight the key points of the following reports, which are closely related to the JSDA: the final report *Recommendations on Valuing Collective Investment Schemes (Revised)* (*1); *Supervisory Toolkit for AI Use in Capital Markets* (*2); consultation report *Regulatory Considerations and Good Practices on the Evolution of Market Liquidity During the Trading Day* (*3); and the report *Extended Trading Hours* (*4).

(*1) *Recommendations on Valuing Collective Investment Schemes (Revised)* (published in June 2026)

<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD824.pdf>

(*2) *Supervisory Toolkit for AI Use in Capital Markets* (published in May 2026)

<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD823.pdf>

(*3) *Regulatory Considerations and Good Practices on the Evolution of Market Liquidity During the Trading Day* (published in March 2026)

<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD824.pdf>

(*4) *Extended Trading Hours* (published in March 2026)

<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD823.pdf>

- The final report *Recommendations on Valuing Collective Investment Schemes (Revised)* consolidates and revises the two valuation principles (*) previously published by IOSCO, taking into account the recent increase in investments in less

liquid and illiquid assets, including private assets, as well as developments in best practices for the valuation of collective investment schemes (CISs). This report proposes new recommendations regarding record-keeping and identifies areas for revision, including governance under market stress, management of conflicts of interest, back testing, use of third-party valuation services, and outdated valuations.

(*) *Principles for the Valuation of Hedge Fund Portfolios* (published in 2007)

Principles for the Valuation of Collective Investment Schemes (published in 2013)

- The main change from the consultation report published in November 2025 is that exchange-traded funds (ETFs) have been included in the scope of the recommendations. When opinions were solicited during the public consultation on whether ETFs should be included, many asset management companies expressed support for this. In addition, many respondents agreed that money market funds (MMFs) should remain out of the scope of the recommendations. Consequently, the final report covers open-end funds and ETFs within the scope of the recommendations, while treating other funds as good practices.
- The final report *Supervisory Toolkit for AI Use in Capital Markets* was prepared to present AI-related considerations to supervisory authorities and to promote effective supervision. This toolkit provides information useful for supervision, including considerations and sample questions in the areas of governance, risk management, outsourcing, disclosure, record-keeping and reporting, and monitoring of AI use.
- The use of generative AI in financial products and services requires more sophisticated supervisory approaches compared to traditional AI systems. It can be difficult to verify the validity of responses generated by generative AI owing to its nature, and specific risks include hallucinations and decision-making biases. The toolkit outlines supervisory considerations regarding such risks, such as whether companies providing services like investment advice have implemented appropriate “human-in-the-loop” mechanisms. As a next step, IOSCO plans to review industry practices regarding disclosure, record-keeping, reporting, and governance related to the use of AI systems in capital markets. To lay the groundwork for this, the toolkit includes a set of questions directed at market participants and others. To ensure that Japan’s specific circumstances are appropriately reflected in future work, we request that the JSDA actively submit its feedback by the deadline of June 26, 2026.

- The consultation report *Regulatory Considerations and Good Practices on the Evolution of Market Liquidity During the Trading Day* analyzes the distribution of liquidity during trading hours, the impact of changes in liquidity patterns and auction designs, and the effectiveness of existing regulations and supervision, based on information from regulatory authorities and exchanges, and presents good practices for maintaining fair and orderly stock markets. Comments may be submitted on or before August 21, 2026.
- The report *Extended Trading Hours* analyzes the benefits and risks of extended trading hours and concludes that after-hours trading is primarily driven by retail investors and is characterized by reduced liquidity and wider spreads compared to regular trading hours. It also points out that regulatory authorities are focusing on assessing whether the existing framework is sufficient to accommodate extended trading hours, and that exchanges are considering risk management and operational measures to mitigate reduced liquidity and execution risks, with key issues including the development of systems and the transition to shorter settlement cycles.
- At the annual meeting, Mr. Toshiyuki Miyoshi, Vice Minister for International Affairs, the FSA, was elected Vice-Chair of the IOSCO Board, following Mr. Shigeru Ariizumi, Vice Minister for International Affairs, the FSA. The FSA will continue to actively contribute to discussions at IOSCO.

2. G7 Finance Ministers and Central Bank Governors Meeting in May 2026

- The G7 Finance Ministers and Central Bank Governors Meeting was held in Paris, France, from May 18 to 19, 2026. Based on the communique released after the meeting, the main points related to the financial sector are as follows.
 - First, members reaffirmed their strong commitment to a stable and resilient financial sector which supports economic growth.
 - Members reaffirmed the Financial Action Task Force (FATF)'s key role, as the global standard-setter, in the fight against financial crime, and called for the effective and timely implementation of the FATF standards by FATF members and the Global Network.
 - On extreme weather events, members noted assessments of the economic and financial impacts of extreme weather events, which can differ across economies,

depending, among other things, on geography and insurance coverage, and underlined the importance of ensuring the availability of robust granular data; enhancing financial literacy; investing in risk prevention; maintaining risk-based regulation and supervision of insurers; and supporting the development of private market capacity.

- On non-bank financial intermediaries (NBFIs), members recognized that, while NBFIs improve capital allocation and diversify funding sources, they may also introduce potential vulnerabilities, and indicated that industry developments and potential risks in the private credit ecosystem call for continued monitoring.
- On cybersecurity, as cyber risks continue to evolve and challenge the resilience of the global financial system, members are committed to take actions to further strengthen their shared response capabilities and to reinforce the preparedness of the financial sector.

○The G7 Summit will be held in Evian, France, from June 15 to 17, 2026. The FSA will continue to communicate with financial institutions and contribute to global discussions.

3. Progress on the formulation of Financial Services Strategy

○As part of its efforts to formulate Japan's Growth Strategy, the government is discussing the Public-Private Investment Roadmap for key products and technologies among the 17 strategic fields in which public-private investment should be specifically promoted, as well as the eight cross-sectoral challenges, including finance.

○With regard to the financial sector, the government plans to formulate a financial services strategy by the summer of 2026, and a draft outline was presented in late April 2026 by Subcommittee (chaired by KATAYAMA Satsuki, Minister of State for Financial Services). Final adjustments are currently underway to formulate the strategy.

○The concept of the Financial Services Strategy is to further advance our initiative to promote Japan as a leading asset management center;

- encourage companies to undertake growth investments that enhance their corporate value over the medium to long term;

- ensure that beneficiaries of asset owners and households can fully share the benefits of economic growth; and
- enable financial institutions and markets to effectively provide funding and growth support that connect these elements.

By doing so, the government will promote growth investment toward the realization of a “strong economy”, and

- ensure that the financial infrastructure can adapt to new technologies.

○ Concrete discussions are still ongoing, measures related to at least the following four pillars may be formulated.

- The first pillar is strengthening the functions of financial institutions and markets to support growth investments in the 17 strategic fields and facilitate corporate transformation and business restructuring. Through regulatory and other reforms of banks and other institutions, the government will support financial institutions in strengthening their funding provision and growth-support functions. At the same time, we will promote the development of deeper and more diverse financial markets. In addition, the government is conducting discussions to further expand and concretize the Regional Financial Power Enhancement Plan, which was developed in December 2025 with the aim of enabling regional financial institutions to contribute to enhancing the value of local businesses and address local challenges.

Furthermore, public-private collaboration regarding financing for the 17 strategic fields is also under discussion.

- The second pillar is corporate governance reform to promote growth investment. The government will push ahead with corporate governance reform to ensure that both companies and institutional investors avoid short-termism, remain strongly focused on sustainable growth and the enhancement of corporate value over the medium to long term, and carry out the necessary growth investments.
- The third pillar is maximizing the benefits of economic growth. The government will encourage asset owners, such as pension funds and universities, to manage their assets in the best interests of beneficiaries, while also working to advance asset management services that support these efforts. In addition, the government

will continue to support steady asset building by households, including through improvement to the DC and iDeCo.

- The fourth pillar is enhancing financial market infrastructure. In addition to working to develop an institutional framework for the implementation and widespread adoption of blockchain-based payment methods and smart contracts, the government will collaborate with the private sector to strengthen cybersecurity measures against AI-related threats in the financial sector.

○ We will work through public-private collaboration.

4. Japan Weeks 2026

○ In 2026, Japan Weeks is scheduled to take place with the period from October 26 to 30 as the core week, and registration for the event began last month.

○ The FSA intends to use this as an opportunity to communicate both domestically and internationally the steady progress of its efforts to transform Japan into a leading asset management center. We hope that the JSDA and its member companies will help promote the appeal of the Japanese market by organizing and participating in events that spark the interest of domestic and foreign investors, thereby further solidifying the progress made to date.

5. Response to unauthorized access and transactions in Internet transactions

○ We understand that many securities companies are working to comply with the implementation of mandatory phishing-resistant multi-factor authentication by the end of this month. However, for securities companies that have not yet finalized a schedule for implementation, we will verify their circumstances based on their respective situations.

○ Where alternative means of multi-factor authentication are provided for unavoidable reasons on the part of customers, securities companies are requested to verify the implementation status of multi-factor authentication and to minimize the risk of unauthorized transactions to the greatest extent possible by strengthening detection functions and implementing additional authentication layers.

○ We would like to ask each securities company to continue to recognize that the management has the responsibilities for security measures and to make every possible

effort to prevent the spread and recurrence of damage for customers.

6. Results of monitoring of securities companies for PY2025

(Major securities companies)

- In recent years, investment products have become increasingly complex and sophisticated, and a wide variety of products are now being offered to customers. It is requested that management work to comprehensively establish the company's business strategies, operational policies, resource allocation, and performance evaluation systems, and build a framework for implementing customer-centric business operations through the PDCA cycle.
- As major securities companies continue to expand their business on a group-wide and global scale, we expect them, under the leadership of senior management, to continue strengthening effective governance and risk management framework commensurate with business strategy.

(Online securities companies)

- We conducted the monitoring of online securities companies regarding the status of their compliance with the revised supervisory guidelines, as well as their customer management systems, including call center operations in light of the increase in inquiries resulting from the rapid increase in the number of accounts and enhanced authentication functions.
- We reiterate that security measures are the responsibility of management, and ask that they make every possible effort to prevent the spread and recurrence of customer damage.

(Mid-sized securities companies and regional securities companies)

- In the current program year, we held in-depth dialogues with top management, mainly from the perspective of building sustainable business models, on the management issues faced by securities companies and their efforts to resolve such issues.
- As a result, many of them cited the following as important issues: maintenance and expansion of the customer base and difficulty in securing human resources due to the declining population, dwindling birthrate, and aging society; the necessity of shifting

to an asset management business model from the perspective of securing stable earnings; and streamlining of middle and back office operations from the perspective of reducing costs.

- We have found that based on the recognition of these issues, securities companies are taking steps to spread customer-oriented business operations, develop and secure human resources, expand their product lineup, and promote digital transformation. We will continue to monitor the status of each securities company's initiatives, etc. through in-depth dialogue.

7. Strengthening Cybersecurity in the Financial Sector Against AI-Driven Threats

- Frontier AI systems have demonstrated a remarkable ability to identify software vulnerabilities and generate sophisticated exploit code. As a result, vulnerabilities that would previously have remained undiscovered for extended periods may be identified at scale and within a much shorter timeframe. There are also concerns that the time between vulnerability discovery and exploitation could shrink significantly. Moreover, the misuse of frontier AI by less sophisticated threat actors may lead to an increase in advanced cyberattacks.
- On April 24, 2026, the Minister of State for Financial Services hosted the Public-Private Coordination Meeting on Strengthening Cybersecurity Measures in the Financial Sector Against AI-Related Threats, which was attended by the Governor of the Bank of Japan, the National Cybersecurity Office (NCO), and the heads of the three megabanks and the Japan Exchange Group. In addition, on May 14, 2026, financial institutions, IT service providers, relevant government bodies, the Bank of Japan, and other stakeholders held a working group meeting to develop a shared understanding of AI-related threats and to examine appropriate measures.
- On 22 May 2026, the FSA and the Bank of Japan jointly called on financial institutions and related entities to take immediate actions in response to the evolving threat landscape associated with frontier AI. Institutions were asked to ensure direct engagement by senior management, including top executives. Financial institutions are expected to move swiftly in implementing the necessary measures, taking into account developments in AI technologies and the activities of AI model providers.
- As part of the government-wide response, the NCO convened an inter-agency

meeting on 18 May 2026 to discuss cybersecurity measures in light of advances in AI capabilities. The meeting adopted a policy package for critical infrastructure operators and issued relevant advisories. Financial institutions, as operators of critical infrastructure, are encouraged to refer to these initiatives when strengthening their own cybersecurity arrangements.

- Looking ahead, AI technologies are expected to continue evolving rapidly. Financial institutions therefore need to move beyond incremental improvements to traditional security measures and reassess their overall approach to cyber defence on the assumption that attackers will increasingly leverage AI. This includes strengthening capabilities for timely vulnerability identification and patch management, enhancing multi-layered defense mechanisms, and improving monitoring and cyber resilience exercises.
- At the same time, the emergence of frontier AI does not render existing cybersecurity measures obsolete. On the contrary, effective implementation of more advanced responses depends on the consistent and timely execution of fundamental cybersecurity practices. In addition, recognizing that no defensive measure can entirely eliminate cyber risk, financial institutions should review their business continuity plans (BCPs) and crisis communication arrangements, and establish clear decision-making processes for responding to periods of heightened cyber threat. Senior management should take a leading role in determining response strategies and ensuring that the necessary resources, including budget and personnel, are made available.

8. Publication of the research report on strengthening third-party cybersecurity risk management at financial institutions

- On April 3, 2026, the FSA published the *Research Report on Strengthening the Management of Third-Party Cybersecurity Risks by Financial Institutions*. This report examines the management practices and other aspects of third-party cybersecurity risk management, an issue of growing importance, adopted by major banks and large insurance companies in the United States, the European Union, and the United Kingdom.
- Financial institutions are expected to enhance their third-party risk management, taking into account the findings and recommendations of this report.

(Reference) A “third party” refers to another organization with which an organization has a business relationship or contract for the purpose of providing services (e.g., outsourced entities such as system subsidiaries and vendors; cloud and other service providers; business partners such as money transfer operators; and API integration partners).

(End)