Systems Risk Management

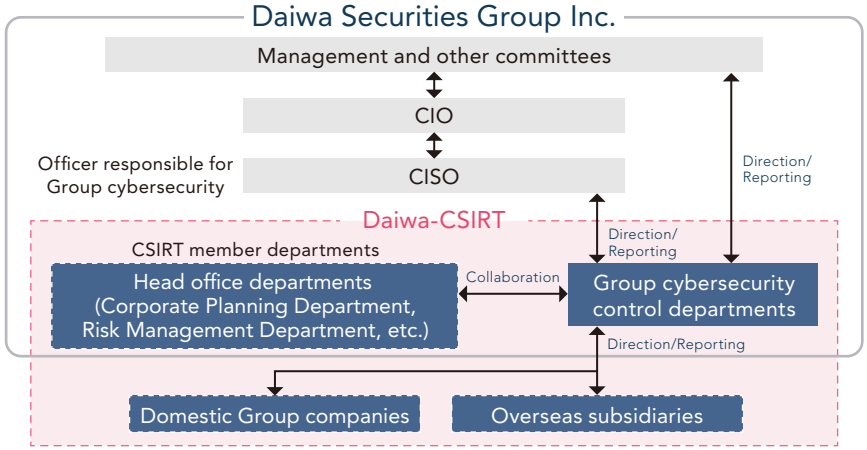
Changes in the environment surrounding financial institutions have made risks increasingly complex, raising concerns that continuity of critical operations may be difficult to maintain through preventive measures and business continuity plans (BCPs) designed for specific scenarios alone. The Group therefore works to ensure operational resilience, including business robustness and recovery capabilities, based on the assumption that business suspensions may occur despite its best preventive efforts. Built on three pillars, cybersecurity, BCPs, and governance, we are working diligently to provide services that our customers can use with confidence.

Cybersecurity

Both Japan and countries around the world have experienced repeated incidents of serious cyberattacks, which have become increasingly sophisticated and diverse through the use of AI. With the emergence of advanced AI capable of independently identifying vulnerabilities and launching attacks in a short period of time, sophisticated cyberattacks have become a significant and increasingly realistic threat. Such attacks are also borderless and demand a comprehensive response that assumes threats from overseas. Under these circumstances, the Group has positioned cybersecurity as a critical management issue and collaborates with outside organizations in an effort led by Daiwa-CSIRT, a dedicated organization that works throughout the Group, while seeking to enhance our defensive capabilities as well as our resilience in the event of a cyberattack, in an ongoing manner.

In July 2026, we established a new department solely responsible for enhancing cybersecurity management. Similarly, we created the Group Chief Information Security Officer (CISO) position to strengthen the governance framework. These moves have enabled us to identify and manage cyber risk in a centralized manner at the management level and to engage in rapid, effective decision-making while implementing countermeasures.

Under this new framework, we prioritize risks based on their significance and potential impact under a risk-based approach, and are strengthening visibility into cyber risk across the Group, as well as enhancing unified risk management and monitoring across Group companies. We are also strengthening both the incident response capabilities of Daiwa-CSIRT and the governance functions of the dedicated cybersecurity management department in an integrated manner. Through these efforts, we are enhancing cyber resilience across the Identify, Protect, Detect, Respond, and Recover functions.



Moreover, we introduced passkey authentication for online trading in order to provide an environment in which customers can carry out transactions securely. By introducing biometric authentication that does not rely on passwords, we have greatly reduced the risks of phishing and unauthorized access.

Strengthening the BCP Framework

From a business continuity planning (BCP) perspective, we had already completed the construction of a BCP response hub by FY2025 in preparation for earthquakes directly beneath Tokyo and other large-scale disasters. This initiative has successfully diversified risk in terms of geography and strengthened business resilience, in addition to enhancing the continuity of systems in the event of an emergency. In FY2026, we will conduct BCP drills for managers and employees in an effort to further improve BCP effectiveness.

Enhancing Three-tiered Governance (AI, Data, and IT)

Recognizing that AI, data, and IT governance are interrelated and complementary, the Group interprets these together as a form of three-tiered governance and seeks to further strengthen this framework. As far as AI governance is concerned, we formulated and disclosed the Daiwa Securities Group AI Governance Mission Statement, within which we defined seven items: Contribution to Society and Economy through AI, Human-Centered AI, Transparency and Accountability of AI, Appropriate Use and Learning of AI, Compliance with Laws and Privacy Protection, Security and Monitoring of AI, and Governance and Literacy Improvement of AI. Moreover, at the Group AI Governance Committee, the Heads of Compliance, Human Resources, CRO and other relevant personnel engage in multifaceted discussions on AI provision, utilization and risk control.

To ensure the safe and efficient deployment of AI agents, we will implement a host of measures going forward. This includes putting in place an integrated management platform, managing the quality of the data we handle, managing access control, and monitoring behavior.

For information regarding the Group's AI governance, please see the website below.
https://www.daiwa-grp.jp/english/about/governance/ai_governance.html