Risk Management at the SBI Group

Risk Management in Support of Enhanced Corporate Value

The SBI Group has based its approach to business management and risk management on the concept of "risk appetite," which can be defined as the types and levels of risk that can be accepted in order to realize strategies. Therefore, the Group sees its risk management role as identifying measures to avoid business disincentives and negative impacts on society while maintaining the Group's growth potential and providing these measures as a source of management decisions for the Board of Directors. One of the features of our approach to risk management is that the level of contribution to the pursuit of its business strategy is recognized as an important aspect of the role of risk management and is therefore reflected in our risk management KPIs.

The Group manages risk factors according to its business fields and regions, given the diversity of its businesses, and implements measures tailored to the nature of each Group company. In addition, the importance of geopolitical risk has grown significantly in recent years, and the perspective of how geopolitical risk affects various risks that are linked to specific financial affairs, growth potential, and reputation is also an important theme of risk management.

A Risk Management System that Is Instrumental to Timely Business Decisions

The Group Risk Management Department forms the core of the Group's risk management system. It comprises, in addition to employees of SBI Holdings, employees of the Group companies such as those seconded from the SBI Shinsei Bank Group and SBI SECURITIES. A special feature is that the department incorporates a wide variety of viewpoints based on the Group's strategy and culture as well as the business characteristics of the banking and securities businesses.

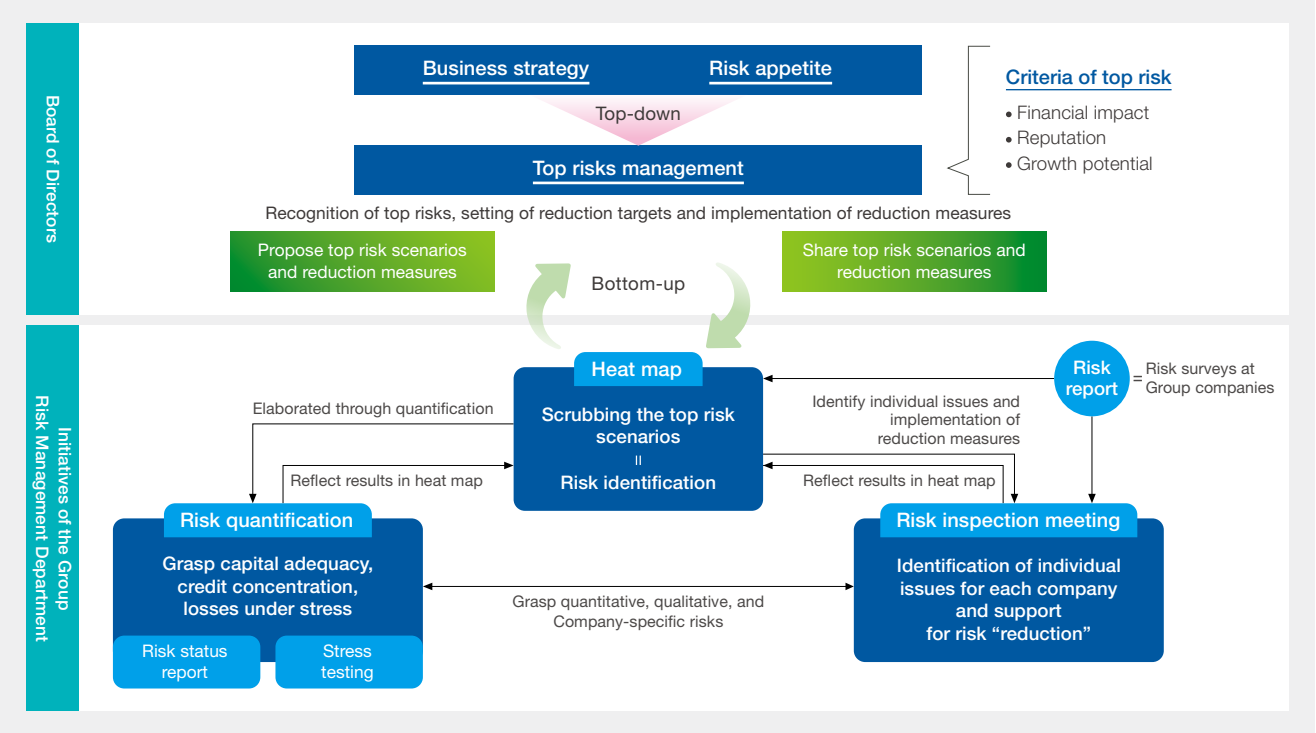
The Risk Management Department also promotes close collaboration with other departments to improve effectiveness of risk management. It consults with the Accounting Department, Financial Department and Sustainability Promotion Office, the Legal Department, the Group Governance & Compliance Department and the IT Management Department on matters relating to information security risks and system risks. Detailed information is shared on a weekly basis, focusing on changes that could affect Group risk, and a system has been established to timely reflect this information in business strategy. Risk management plans are reported to the Board of Directors each period and progress reports are reported twice a year. Additionally, quantitative reports on risk information are presented separately each quarter.

Risk Identification Process

In managing risks of the SBI Group which encompasses a diverse range of businesses, we make regular updates on our group-wide "top risks."

We identify the top risks by using a top-down approach

Big Picture View of the Group Risk Management Department



Frequency [Annually] Risk report [Quarterly] Risk status report [Monthly and ad hoc] Risk inspection meeting

based on a broad risk scenario that is assumed from the business strategy for each period. We also adopt a bottom-up approach for each business field involving various indicators for each risk category, such as market, credit and operational risk, in order to identify items that are assumed to be high risk. As a result, these two approaches allow us to identify various top risks, such as information security, losses due to uncertain market conditions, capital management, system failure due to tight capacity, etc., and report on them for effective mitigation and management decision-making on the scope of risk appetite.

The Three Pillars of Risk Management

The three pillars of our broad-sweeping, comprehensive risk management are methods of heat maps, stress tests, and risk assessment meetings.

The heat map is a graphical representation of the results of quantitative risk indicators and qualitative risk information collected from Group companies. It is prepared on a regular basis in accordance with risk assessment meetings and various risk status reports from subsidiaries.

Stress tests are mainly conducted in fields that lend themselves to quantitative risk management and are designed to calculate what type of financial losses may be incurred under stress scenarios.

A risk assessment meeting is an initiative that lessens risks carried by the Group while also supporting Group companies by providing advice and guidance on their internal control systems. This method starts by selecting Group companies for priority monitoring and holding separate dialogues with individual companies to get a concrete grasp of risks. Unlike the other two methods which involve broadly scoped management targets considered from a holistic view, the risk assessment meeting uses individualized micro points of view.

A multidisciplinary combination of these methods enables risk management that is both big-picture and dynamic, while not leaving out any individual issues.

Cybersecurity at the SBI Group

SBI Group's Cybersecurity System

The SBI Group recognizes cybersecurity as one of its highest management priorities and has established the "SBI Group Security Guidelines" and the "SBI Group Cybersecurity Standard." In 2023, we also established the "SBI Group Guidelines for the Use of Generative AI" to ensure security and to protect confidential information in the use of generative AI. These guidelines are reviewed regularly.

The SBI Group's cybersecurity system is overseen by the Information Security Officer at SBI Holdings, who serves as the Group Information Security Manager. The IT Management Department plays a central role in implementing information security measures across the Group. Furthermore, the SBI Group Computer Security Incident Response Team (CSIRT) is also set up, with the IT Management Department serving as its secretariat. The CSIRT holds monthly liaison meetings with Group Information Security Managers and experts in the Group to prevent security incidents by analyzing latest threat trends and to enhance SBI Group's resilience such as minimizing damage. Also, in order to raise the overall level of cybersecurity across the Group, we hold four cybersecurity liaison meetings per year where information is shared among information security managers at Group companies.

In the event of an incident, a joint response is coordinated by the IT Management Department, which specializes in IT-related matters including responses to cyberattacks, and the Group Risk Management Department, which oversees overall risk management. The two departments maintain close, ongoing collaboration, including biweekly information-sharing, to strengthen multilayered and comprehensive security management. Regular reports are also made to the Board of Directors.

Developing Human Resources for Enhanced Cybersecurity

The SBI Group provides training programs on cybersecurity countermeasures for all company officers and employees, and invites external experts to provide training for management. In addition, the Board of Directors holds regular discussions on cybersecurity education. For those engaged in systems operation and management at Group subsidiaries, seminars are regularly held inviting outside lecturers. In addition, an information-sharing portal dedicated to cybersecurity is used, which helps leveling out biases in knowledge regardless of a company's size or field of business. All SBI Group employees are required each year to participate in e-learnings to build a sense of ethics and share knowledge.

Maintenance of Cybersecurity

The SBI Group comprises companies of diverse sizes and maturity levels, resulting in potential disparities in cybersecurity frameworks, human resources, and accumulated knowledge. We recognize the need to address these imbalances and strive for a more standardized approach to cybersecurity across the Group. In recent years, state-sponsored threat actors have become an increasingly visible force in cyberattacks around the world, with the financial sector being a particularly frequent target. In response, we have built a Group-wide common security platform that incorporates threat intelligence and the zero-trust security model, enabling a rapid and flexible response to signs of incidents and related risks at each Group company. We believe that the establishment of a management framework like this is an effective method for putting in place a cybersecurity system at a Group characterized by the persistence of discontinuous growth. In our quest for developing Company initiatives that can be horizontally applied as Group-wide countermeasures, we are strengthening our detection and monitoring while carrying out constant surveillance to spot signs of an incident (including DDoS attacks, ransomware attacks, data breaches, and malware infections) so that we can take a rapid response against such threats.

In recognition of these initiatives, SBI Holdings was certified as a company with an excellent, proactive attitude and cybersecurity information disclosure in the Cyber Index Company Survey 2024, published by the Information Technology Federation of Japan on January 9, 2025.