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.

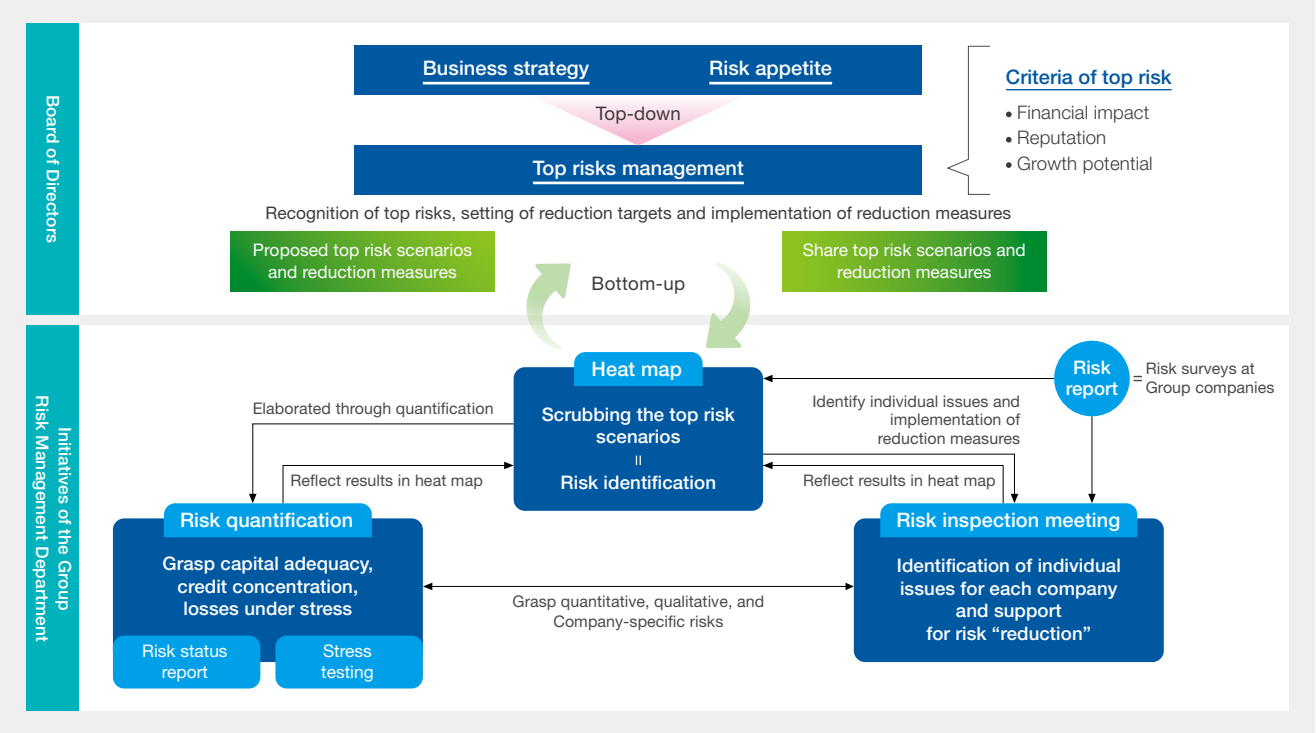
The Risk Management Department also promotes close collaboration with other departments to improve effectiveness of risk management. It consults with the Accounting Department, Financial Department and Sustainability Promotion Office, the Legal Department, the Group Governance & Compliance Department 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. ➡ P.47

Risk Identification Process

Because the Group encompasses a diverse range of businesses, we can only manage risks within the Group by making regular updates on our "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 employ a bottom-up approach 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, rising interest rates, capital management and systems, and country risks, 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 enhancement of cybersecurity is one of the Group's most important management issues. We are working to strengthen our comprehensive cybersecurity preparedness under the SBI Group Cybersecurity Standard, which we formulated to apply to the entire Group. In 2023, we also began to apply the "SBI Group Guidelines for the Use of Generative AI" as a framework for ensuring security and protecting confidential information whenever generative AI is used.

The SBI Group's cybersecurity system is overseen by the Executive Officer of SBI Holdings, who is the Group Information Security Manager with the IT Management Department as the core of its operation. Furthermore, the SBI Group Computer Security Incident Response Team (CSIRT) is also set up under the IT Management Department. 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 through rapid incident response.

SBI Group companies vary significantly in terms of their business fields and the scale of their activities. We therefore hold four cybersecurity liaison meetings per year to raise the overall level of cybersecurity across the entire Group. These meetings, which are attended by information security managers and employees from each SBI Group company, are an opportunity to share information on cybersecurity measures, trends, and other relevant topics across the Group.

The IT Management Department and the Group Risk Management Department work closely together on a regular basis. For example, they share information every other week, and in the event of an incident, they work together to implement a join response plan. The IT Management Department, which specializes in IT security including counter cyberattacks, and the Group Risk Management Department, which manages general risks, collaborate to bolster security comprehensively and on multiple levels.

Developing Human Resources for Enhanced Cybersecurity

The SBI Group provides training programs on cybersecurity countermeasures for all 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 to participate in e-learning on cybersecurity to build a sense of ethics and share knowledge.

Putting in Place Cybersecurity That Encompasses the Whole Group

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. As digitalization progresses, cyberattacks are becoming more ingenious and sophisticated, making it difficult to provide complete protection against cyber-incidents just using the existing arsenal of measures. We have therefore established a Group-wide common security platform that adopts the zero-trust security concept, constructing an environment in which individual Group companies can respond dynamically against indications of an incident and their risks. 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 recognition of these initiatives, SBI Holdings was certified as one of 44 companies with an excellent attitude and cybersecurity information disclosure in the Cyber Index Company Survey 2023, published by the Information Technology Federation of Japan on December 8, 2023.