Feature

Attaining Appropriate Risk Management for Executing Management Strategy

Risk Management at the SBI Group

Risk Management in Support of Enhanced Corporate Value

At the SBI Group, which has achieved sustainable growth ever since its founding, the idea of business management and risk management based on risk appetite (what risks are taken and to what extent in order to realize the strategy) has taken root. 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 basis for management decisions. The Group recognizes that contributing to the promotion of its business strategy is an important role of risk management, and the Group's risk management is characterized in that it places the degree of contribution as an indicator for risk management KPIs.

The Group manages risk factors according to its business areas and regions, given the diversity of its businesses. Due to the reorganization of our current business segments, we have been able to develop measures tailored to the nature of the business, including risk management. In addition, the importance of geopolitical risk has increased 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, which forms the core of the Group's risk management system, comprises, in addition to employees of SBI Holdings, employees of Group companies in the financial business, such as those seconded from the SBI Shinsei Bank Group and those concurrently working for 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 collaboration with other departments: in accounting and finance, it works with the director in charge of accounting and finance, who is also in charge of the department; in sustainability risk, with the Sustainability Promotion Office; and in compliance, with the Legal & Compliance Department. In addition, information security risks and system risks are addressed in cooperation with the IT Management Department.

Also, the officers responsible for risk management and the Department maintain a system that enables close reporting and information sharing from time to time. In other words, detailed information is shared at flexible timings, such as weekly, focusing on matters where there have been some 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.45

Risk Identification Process

The Company has developed a mechanism in which regular updates are made to the "top risks," a set of risks that span across the entire Group. These risks have been identified for the purpose of managing risk within the Group, which encompasses a diverse range of businesses.

In order to identify the top risks with major impacts upon the Group's growth potential, reputation, and finances, the Company adopts both a top-down and a bottom-up approach. In the top-down approach, a broad risk scenario is assumed from the business strategy for each period. In the bottom-up approach, various indicators for each risk category, such as market, credit and operational risk, are compiled for each business type, and items that are assumed as high-risk are identified. The Company has identified, for example, rising interest rate risk, regulatory risk, system risk and cybersecurity risk in Internet business as the top risks and reported on them for effective mitigation and management decision-making on the scope of risk appetite.

The Three Pillars of Risk Management

In order to have this type of broadsweeping, comprehensive

risk management, the Company utilizes the risk management methods of heat maps, stress tests, and risk inspection meetings as the three pillars.

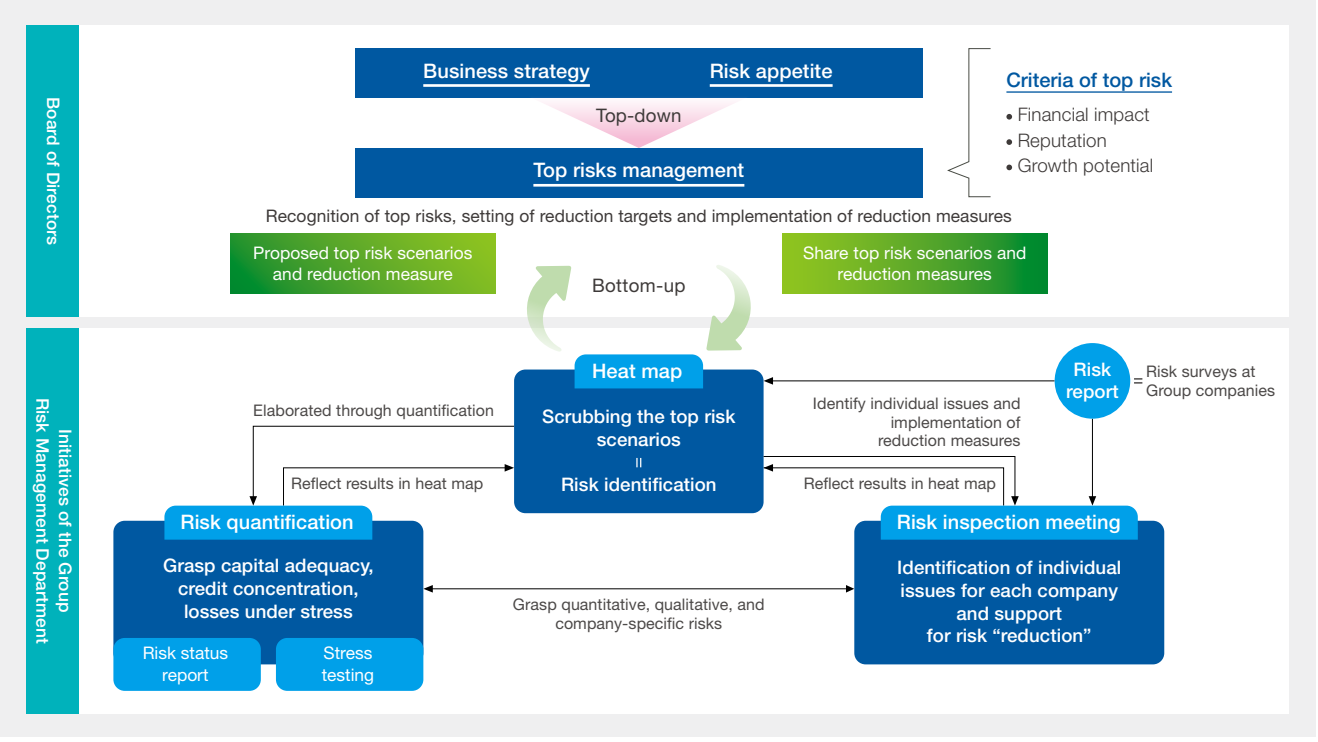
The heat map is a graphical representation of the results of various quantitative risk indicators and qualitative risk information collected from Group companies in accordance with their business type from a Group perspective. The Heat map is prepared on a regular basis in accordance with risk inspection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

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

A risk inspection meeting is an initiative that lessens risks carried by the Group while also supporting subsidiaries by providing advice and guidance on their internal control systems. This method starts by selecting subsidiaries 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 inspection meeting uses individualized micro points of view.

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

Big Picture View of the Group Risk Management Department



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

Cybersecurity at the SBI Group

The SBI Group's Cybersecurity System

As a pioneer of Internet financial services in Japan, the SBI Group considers the enhancement of cybersecurity to be one of its most important management issues.

The Company, which has financial businesses within the Group – namely securities, banking, and insurance – has specified the SBI Group Cybersecurity Standard, which is a set of guidelines that apply to the entire Group. The SBI Group Cybersecurity Standard is based on various cybersecurity frameworks including the FISC Security Guidelines for the construction of information systems by financial institutions, the framework from the National Institute of Standards and Technology (NIST) in the U.S., and the international cybersecurity standards known as the CIS Controls. This Standard has bolstered our comprehensive cybersecurity policy.

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 CSIRT (Computer Security Incident Response Team) is also set up under the IT Management Department. The SBI Group CSIRT holds monthly meetings and also collaborates with external experts in cybersecurity, communicates with internal depart-

ments and subsidiaries, and shares information with the Financial Information Sharing and Analysis Center (FISC), as well as the Japan Cybercrime Countermeasures Center (JC3). Through these measures, the SBI Group CSIRT works to enhance SBI Group's resilience by preventing security incidents by analyzing latest threat trends and minimizing damage through rapid incident response.

The SBI Group holds four cybersecurity liaison meetings per year, attended by information security managers and persons responsible for information security among Group companies. These meetings are an opportunity to share information on cybersecurity measures, trends, and other matters across the Group. We recognize that these meetings are vital for raising the overall level of cybersecurity across the Group, as the size and scope of businesses vary from company to company.

Regarding collaboration with related internal departments, the IT Management Department and the Group Risk Management Department share information on a weekly basis. In the event of an incident, the two departments work together to implement a joint response plan. The departments have a close working relationship and communicates regularly. 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.

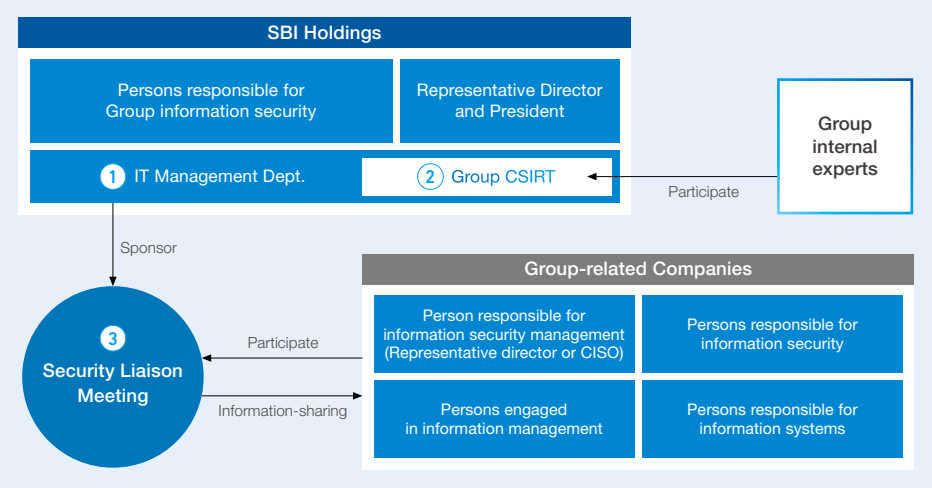
Developing Human Resources for Enhanced Cybersecurity

We believe that cybersecurity policy is not just for IT specialty departments, but rather, that it is essential that all employees understand the importance of cybersecurity and take preemptive measures on a regular basis. The Group has implemented a cybersecurity training program for the entire company, including the management team and individual managers; those engaged in development and operation of IT systems; those who plan, promote, or administer services; and employees involved in sales and operations. For those in the management level, external experts are invited to visit and conduct training, and the Board of Directors regularly discusses and deliberates on cybersecurity issues at its meetings. 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 to communicate calls for vigilance about vulnerabilities and steps and countermeasures to be taken, which helps leveling out biases in knowledge regardless of a company's size and field of business. For employees, the Company offers training against phishing emails and raises awareness towards risks of cyberattacks, as well as making e-learning on cybersecurity mandatory, which is essential for building a sense of ethics and sharing knowledge about the latest cybercrime, countermeasures, and how to deal with them.

Putting In Place Cybersecurity That Encompasses the Whole Group

For the Company group, which promotes advanced and diverse businesses and includes companies of various sizes and maturity levels, the presence of imbalances in cybersecurity frameworks among these companies, or in human resources and accumulated knowledge, is seen as a Group issue. Also, as digitalization progresses, cyberattacks are becoming more ingenious and sophisticated, making it difficult to provide complete protection against cyber-incidents using the existing arsenal of measures. As a measure to address these challenges, the Group has been constructing a common security platform that adopts the zero-trust security concept. By making use of this platform, individual companies are constructing an environment that enables a dynamic response against indications of an incident and their risks. The erection of a management framework like this is recognized as an effective method for putting in place a cybersecurity system at a Group characterized by the persistence of discontinuous growth.

Outline of Cybersecurity System



Overview of main organizations

1. Manages cybersecurity for the overall Group
2. CSIRTs are formed across the Group, including participants from Group companies in the financial realm
3. A meeting for sharing information on cybersecurity across the entire Group