1 Basic Policy on Risk Management

In order to ensure sound management, secure revenue through risk taking based on management strategies, and achieve sustainable growth, the Group follows a basic policy of accurately assessing risk conditions and implementing necessary risk-related measures through a series of risk management activities, including risk identification, evaluation, monitoring, control and mitigation, validation for advancement, and review, based on the Group's management policy and basic policy on the internal control system.

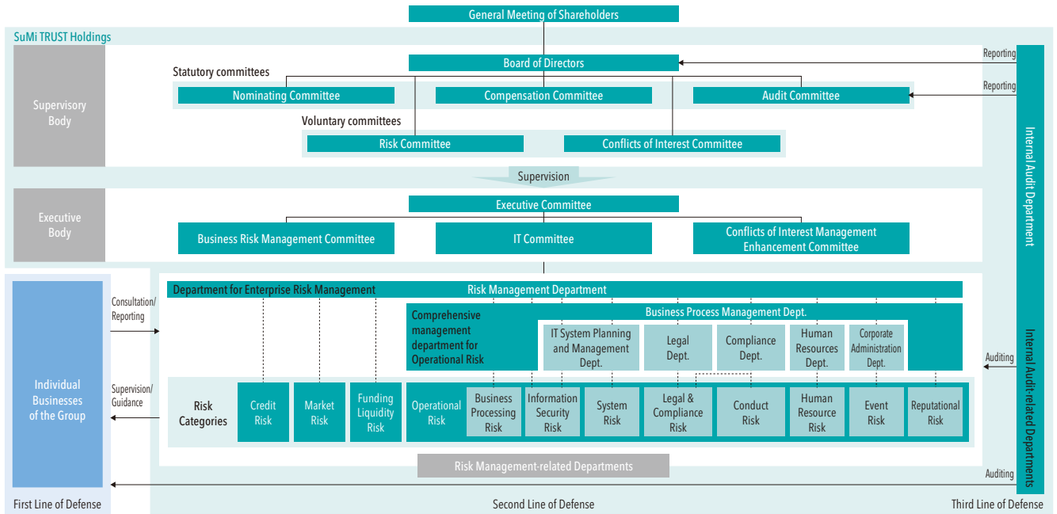
The Group's risk management framework encompasses the Risk Appetite Framework, and integrates it to function organically within the Group.

2 Risk Management System

(1) Risk Governance System

For the group-wide risk governance system, the Group has developed a Three Lines of Defense system consisting of risk management by individual businesses (first line of defense), risk management by the Risk Management Department and individual risk management-related departments (second line of defense), and validation by the Internal Audit Department (third line of defense).

■Risk Governance System



1) First Line of Defense

Each Group business identifies and gains an understanding of the risk characteristics involved in carrying out its own business, based on knowledge of the services and products in that business. Each business takes risks within the scope of its risk appetite (the type and amount of risk to be taken to achieve the goals set in the management plan) in accordance with its risk-taking policy, evaluates risks, and swiftly implements risk control at the on-site level when risks materialize. In addition, the status of risk management is reported to the second line of defense in a timely manner.

2) Second Line of Defense

The Risk Management Department and risk management-related departments act as control departments responsible for the management of each risk category. In accordance with the Group-wide basic policy on risk management approved by the Board of Directors, the Risk Management Department and risk management-related departments act as a check-and-balance function for the risk taking of the first line of defense, and supervise and provide guidance regarding the risk governance system from an independent standpoint.

The Risk Management Department, as an Enterprise Risk Management Department, performs overall risk management, identifies and evaluates group-wide risks, creates a risk management process, and sets risk limits in accordance with the group-wide risk management policy determined by the Board of Directors. In addition, it formulates group-wide recovery strategies, in advance, to prepare for cases when risks materialize. Furthermore, it shares information with risk management-related departments appropriately, monitors the overall status of risks and risk management in an integrated manner, and reports the status to the Executive Committee and the Board of Directors.

3) Third Line of Defense

The Internal Audit Department audits the effectiveness and appropriateness of the group-wide risk governance system and processes from a standpoint independent of the first and second lines of defense.

4) Executive Committee

The Executive Committee is composed of representative executive officers and executive officers designated by the President. It makes decisions on matters concerning risk management and undertakes preliminary discussions regarding matters to be resolved by and reported to the Board of Directors.

5) Board of Directors

The Board of Directors is composed of all of the directors. It decides on the Group's management policy and strategic goals for risk taking, formulates a risk management policy, etc. that reflects these strategic goals based on a solid understanding of the location and nature of risks, and develops an appropriate risk governance system and supervises its implementation. The Board of Directors has voluntarily established the Risk Committee and the Conflicts of Interest Committee, as advisory bodies, based on the business strategies and risk characteristics of the Group.

- **Risk Committee**

The Risk Committee receives requests for consultation from the Board of Directors on matters concerning the business circumstances surrounding the Group and the effectiveness of its risk management, etc., reviews their appropriateness, and reports its findings.

- **Conflicts of Interest Committee**

The Conflicts of Interest Committee receives requests for consultation from the Board of Directors on matters concerning the Group's fiduciary duties and conflict of interest management, which are the foundation on which the Group seeks to become the "Best Partner" of its clients based on a fiduciary spirit, reviews their appropriateness, and reports its findings.

(2) Risk Management Process

In the Group, the Risk Management Department and individual risk management-related departments act as the second line of defense, performing risk management using the following procedure. This risk management process, along with its associated systems, undergoes regular auditing by the Internal Audit Department, which acts as the third line of defense.

1) Risk Identification

The risks faced by the Group are comprehensively identified, while ensuring the comprehensiveness of the Group's operations, and the risks to be managed are identified based on the scale and characteristics of the identified risks. Of note, risks that are particularly important are managed as material risks.

2) Risk Evaluation

The risks identified as requiring management undergo analysis, assessment, and measurement in a manner appropriate for the business scale, characteristics, and risk profiles. We periodically evaluate material risks in terms of frequency of occurrence, degree of impact, and severity to determine whether they can be classified as "top risks" (risks that require management attention due to their potential to have a material impact on the Group's business capabilities and earnings targets within one year) or "emerging risks" (risks that could have a material impact in the medium to long term; i.e., after one year).

3) Risk Monitoring

After setting KRIs* and other indicators, risk conditions are monitored with appropriate frequency, given the conditions of the Group's internal environment (risk profiles, allocated capital usage status, etc.) and external environment (economy, markets, etc.). Recommendations, guidance, and advice are given to each of the Group's businesses based on the risk conditions. Monitoring contents are reported and submitted to the Board of Directors, the Executive Committee, and other bodies regularly or as needed.

* KRI = Key Risk Indicator

Risk Predictor Management for Top Risks, etc.

Risk appetite indicators are defined for risks resulting from internal factors, based on the features of the Group's business model and risk characteristics, and these management indicators are monitored. Regarding risks resulting from external factors, the top risks and emerging risks are selected, and risk predictors are monitored. Countermeasures are implemented based on the monitoring results for both types of risks.

The top risks and emerging risks at present include "Risks related to the global COVID-19 pandemic", "Risks related to climate changes", and other risks. The results of risk analysis and necessary countermeasures are reported to the Board of Directors and the Executive Committee.

■Main Top Risks and Emerging Risks

Risks related to the COVID-19 pandemic
Risks related to falling prices for strategic shareholdings and similar assets
Risk related to concentration of credit in major obligors in the credit portfolio
Risks related to cyberattacks
Risks related to climate change*
Risks related to emergence of geopolitical events (e.g. the Ukraine crisis)
Risks related to innovation
Risks related to Japan's declining birthrate and aging population

* Please refer to the section of this report titled Addressing Climate Change Issues and to the TCFD Report 2021/2022 (published in January 2022) for information on the Group's efforts to counter risks related to climate change.

4) Risk Control and Mitigation

If any incidents that could have a significant impact on the soundness of management occur, such as the risk amounts exceeding the risk limits, or the existence of concerns that it might do so, appropriate reports are presented to the Board of Directors, the Executive Committee, and other bodies, and the necessary countermeasures are implemented according to the severity of the risk.

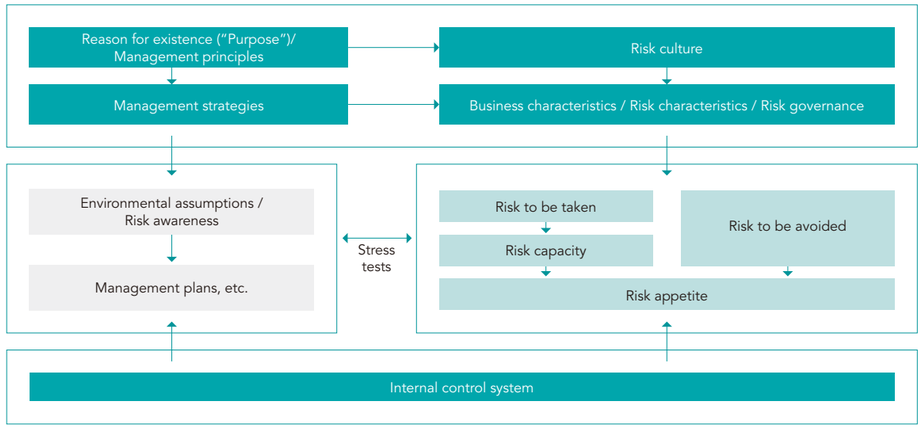
3 Risk Appetite

(1) Outline of the Risk Appetite Framework

The Risk Appetite Framework (RAF) is a group-wide corporate management framework consisting of the process for determining risk appetite within the Group's risk capacity, in order to achieve management strategies formulated based on the Group's reason for existence ("Purpose") and management principles ("Mission"), together with an internal control system that monitors the process and ensures its appropriateness and sufficiency.

To improve profitability and enhance risk management, the Group's RAF establishes communication processes through the setting, propagation, and oversight of risk appetite and promotes the improvement of transparency in the decision-making process, the optimization of management resource allocation, and the strengthening of the monitoring system for the whole of risk-taking.

■Outline of the Risk Appetite Framework



(2) Risk Appetite Controlling Process

1) Determining Risk Appetite Target

The Group classifies risks into two categories: (1) risk to be taken (that occurs in relation to activities that generate returns) and (2) risk to be avoided (such as conduct risk that cannot be tolerated by the Group).

Under RAF, the Board of Directors establishes a risk-taking policy, which is an overriding management policy based on its management principles, and takes into account the results of stress tests to set risk appetite indicators. In addition, the Executive Committee sets more detail risk-taking policy and risk appetite indicators for each business within the scope of policy set by the Board of Directors.

The risk-taking policy and risk appetite indicators are determined in accordance with the management plan, and are reviewed at least once a year or when necessary.

2) Monitoring of Risk Appetite Tolerance

In order to verify that risk taking is conducted appropriately based on its business model, the Group sets separate risk appetite indicators from the three perspectives of return, risk, and cost, and monitors them regularly. If the indicators deviate from the set levels, the Group analyzes the cause and implements countermeasures or reconsiders the levels of risk taking.

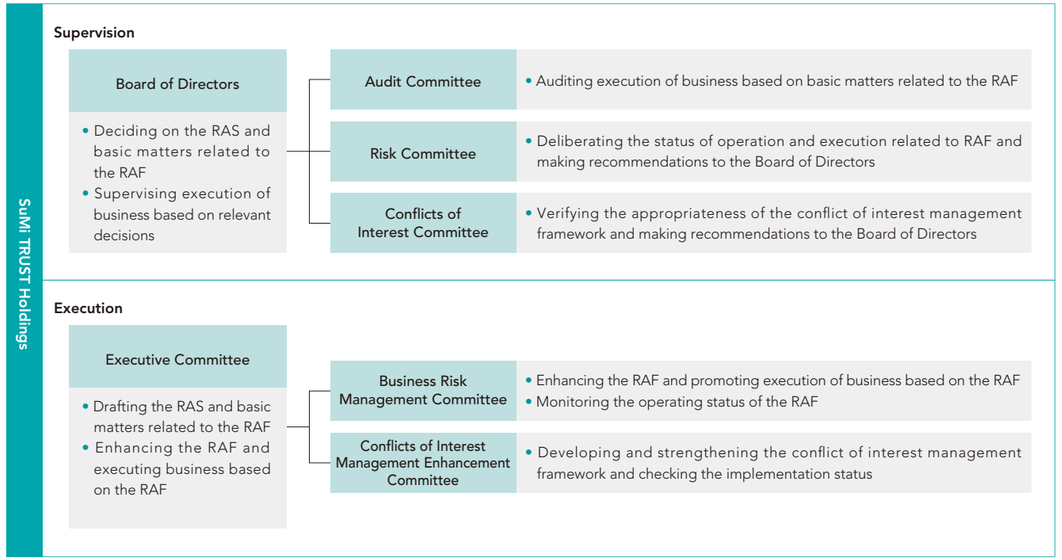
3) Risk Governance

Risk governance, which forms a part of corporate governance, is a framework for identifying, measuring, managing, and controlling risks, as well as ensuring appropriate risk taking, by defining and monitoring risk appetite.

The Group promotes the enhancement of risk governance, with the aim of achieving the sustainable and solid development of the Group.

The Group is working on enhancing the operation of risk appetite through discussions at the Risk Committee and the Conflicts of Interest Committee, etc. as part of its initiatives to enhance corporate governance.

■Risk Appetite Framework Management System



(3) Developing Positive Risk Culture

The Group defines risk culture as a basic philosophy that prescribes the codes, attitudes, and conduct of the Group, as well as its directors, officers, and employees, that flexibly execute risk taking, risk management, and risk control based on an appropriate assessment of risks, guided by a high degree of self-discipline based on the fiduciary spirit.

In order to foster a risk culture so that it will take root across the Group, we define risk-taking policies for each business when formulating its management plan, and encourage appropriate risk-taking by all officers and employees. In this way, the Group aims to build sustainable business models that contribute to increasing corporate and stakeholder value. In addition, we have formulated a Risk Appetite Statement (RAS) clearly stating our RAF, which is used as a common language in lively discussions concerning risk appetite within the Group.

4 Risk Characteristics

Based on a fiduciary spirit, and leveraging its significant expertise and comprehensive capabilities, the Group, as a trust bank group, strives to create distinct value through a total solution business model that combines its banking, asset management and asset administration, real estate businesses, and others.

The Group faces various risks, including credit risk, market risk, funding liquidity risk, and operational risk, which vary depending on the business characteristics of each of the Group's businesses.

In this context, as a basis for improving management of risks related to trust business operations, we have established Group-wide Trust Business Guidelines to provide information about basic matters that warrant caution. SuMi TRUST Bank primarily manages these risks in the operational risk category, particularly in terms of its duty of due care as a prudent manager, duty of loyalty, and duty to segregate property as a trustee.

Reporting is regularly performed regarding whether the overall risk of the Group, combining the risks of each business, is within the limits of risk capacity (soundness and liquidity) that have been determined by the Board of Directors.

■Risk Definition

Risk Category	Definition
Credit Risk	Risk that the Group may incur losses due to a decrease or impairment of the value of assets (including off-balance sheet assets), for reasons such as deterioration of the financial condition of obligors. In this regard, "country risk" in particular refers to the risk that the Group may incur losses on credit provided overseas, due to the foreign exchange, political, or economic conditions in the countries where our clients operate.
Market Risk	Risk that the Group may incur losses due to fluctuations in the value of assets/liabilities (including off-balance sheet assets/liabilities), or in the earnings generated from assets/liabilities, due to fluctuations in various market risk factors, such as interest rates, foreign exchange rates, stocks, commodities, and credit spreads. In this regard, "market liquidity risk" in particular refers to the risk that the Group may incur losses due to a situation in which it becomes impossible to conduct transactions in the market, or becomes obligatory to trade at prices that are significantly more disadvantageous than usual, due to market turmoil.
Funding Liquidity Risk	Risk that the Group may incur losses in a situation where it becomes impossible to secure necessary funds, or becomes obligatory to raise funds at interest rates significantly higher than usual.
Operational Risk (Below are "risk sub-categories" within Operational Risk)	Risk that may adversely affect the Group, clients, markets, financial infrastructure, society, or the work environment due to inadequate or failed business processes, the activities of executives or employees, computer systems, or due to external events.
Business Processing Risk	Risk that the Group may incur losses due to inappropriate business procedures arising from executives or employees neglecting to engage in proper business activities, or other incidents such as accidents or fraud.
System Risk	Risk that the Group may incur losses due to reasons such as computer system failures, malfunctions, and defects, as well as the risk that the Group may incur losses due to unauthorized computer usage.
Information Security Risk	Risk that the Group may incur losses due to the improper management or maintenance of information assets. This includes information leaks, information errors, and misuse of information, as well as an inability to use the information system.
Legal & Compliance Risk	Risk that the Group may incur losses due to uncertainty regarding the legal aspects of transactions, or due to insufficient compliance with laws, regulations, etc.
Conduct Risk	Risk that may adversely affect the Group, clients, markets, financial infrastructure, society, or the work environment due to the actions of Group companies, executives, or employees that are unprofessional or do not meet the expectations and trust of stakeholders.* *Appropriate service level set by the Group based on an understanding of reasonable expectations
Human Resource Risk	Risk that the Group may incur losses due to personnel and labor management issues, such as unequal or unfair management of personnel, and harassment.
Event Risk	Risk that the Group may incur losses due to external events that impair business, such as natural disasters, crimes such as terrorism, damage to public infrastructure that prevents its functioning, and the spread of infectious diseases, or due to the inappropriate use or management of tangible assets.
Reputational Risk	Risk that the Group may incur losses as a result of a deterioration of the reputation of SuMi TRUST Holdings or its subsidiaries, due to reasons such as mass media reports, rumors, or speculation.

5 Enterprise Risk Management

(1) Enterprise Risk Management System

We manage risks by comprehensively grasping the risks faced by the Group, which are evaluated on an individual risk category basis, and comparing and contrasting them against our corporate strength i.e. capital adequacy (enterprise risk management).

We evaluate the effectiveness of our risk management and risk control annually, and when the need arises due to changes in the business environment or other circumstances, we will consider revisions to our risk category system, risk management system, and other policies.

Among the risks we manage through our enterprise risk management, we combine the risk values for risks that can be quantitatively measured using a single standard, such as VaR*, and compare the combined vale against our corporate strength i.e. capital adequacy, thereby managing risks (integrated risk management).

* VaR = Value at Risk

(2) Capital Allocation Operations

For the purpose of the Group's capital allocation operations, SuMi TRUST Holdings allocates capital to each business, including the Group companies, based on each risk category (credit risk, market risk, and operational risk) in consideration of the external environment, risk-return performance status, scenario analysis, and the results of assessments of capital adequacy levels. The capital allocation plan is subject to the approval of the Board of Directors. Capital allocation levels are determined based on the Group's risk appetite.

Each business is operated within both the allocated amount of risk capital and its risk appetite. The Risk Management Department measures the risk amount on a monthly basis, and reports regularly on the risk conditions, compared to the allocated capital and risk appetite, to the Board of Directors, and others.

(3) Stress Tests and Assessment of Capital Adequacy Level

The Risk Management Department performs three types of stress tests (hypothetical scenario stress testing, historical scenario stress testing, and examination of probability of occurrence) each time a capital allocation plan is formulated or reviewed, with the aim of ensuring capital adequacy from the standpoint of depositor protection. Based on the results of these stress tests, it assesses the level of capital adequacy, and reports to the Board of Directors, and others.

6 Information Security Risks and Cybersecurity Measures

SuMi TRUST Group considers information assets to be one of the most important managerial resources, and has set the protection of personal information and customer data as one of the management foundation materialities. In addition, the Group also identifies information security risk as "Risk that the Group may incur losses due to the improper management or maintenance of information assets, including through information leaks, information errors, and misuse of information, as well as an inability to use the information system," and positions it as one of the risk subcategories under operational risk. It has assigned an officer in charge and established a control department to properly manage customer information and implement cybersecurity measures.

In addition, we have established and announced our Declaration for the Protection of Personal Information, which is a set of policies designed to ensure the protection of the personal information of our clients and shareholders, and have declared to abide by them.

We will establish internal rules regarding the management framework and handling of information in accordance with the Personal Information Protection Act, related laws and regulations, and the "Guidelines for Personal Information Protection in the Financial Field" established by the Financial Services Agency. We will also hold regular training sessions for all employees twice a year to ensure that they are fully acquainted with the points of concern regarding the handling of information in their daily operations and to promote a principles-based understanding of information security.

(1) Organizational structure, etc.

Matters related to information security risk, as a risk subcategory within operational risk, are deliberated comprehensively by the Business Risk Management Committee at SuMi TRUST Holdings and by the Operational Risk Management Committee at SuMi TRUST Bank, covering a series of processes such as the development of a management framework, formulation of plans, and the identification, evaluation, monitoring, and control of risks. In addition, policies and plans are decided by the Board of Directors after deliberation by the Executive Committee.

Based on the rules regarding authority, the series of processes are executed by the Business Process Management Department, the IT System Planning and Management Department, and other control departments responsible for information security risk management. The officer in charge of the Business Process Management Department and the officer in charge of the IT System Planning and Management Department are responsible for overall information security risk management.

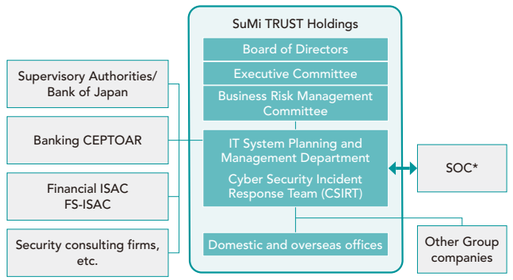
(2) Cybersecurity Management Framework

The Group has designated cyber-attacks as one of the governance and management framework materiality as well as a top risk, and has formulated the "Cybersecurity Management Declaration" to plan and promote cybersecurity measures under the leadership of our management team.

- We have established SuMiTRUSTCSIRT as a specialized organization for cybersecurity measures, and have built a management framework that collects and analyzes threat and vulnerability information from within and outside the Group, plans and implements security measures, and reports to management. We are also promoting the advancement of security measures through security review meetings and our IT Committee, as well as by utilizing outside expertise.
- The Group has established internal rules and regulations based on US security standards, and has developed processes for responding to cyberattacks both in normal times and in emergency situations.

- In addition to conducting cybersecurity risk assessments and system vulnerability assessments on a regular basis for SuMi TRUST Group and its subsidiaries and affiliates, we are promoting the standardization of cybersecurity rules and regulations to enhance and standardize the cybersecurity framework for the Group as a whole.

■Cybersecurity Management System



* Security Operation Center (SOC): The organization that monitors networks to detect and analyze cyberattacks.

(3) Monitoring System

The Group has built a common infrastructure for internet communications, and the Security Operation Center (SOC) monitors the common infrastructure network 24 hours a day, 365 days a year and detects threats by conducting correlation analysis of various types of data. This information is consolidated in SuMiTRUST-CSIRT*1, and we have established a monitoring system centered on the CSIRT.

(4) Enhancing Cybersecurity Measures

We have established perimeter defense measures (multi-layered defense consisting of entry, exit, and internal measures) as a technical countermeasure against cyberattacks, and are working to reduce risk by implementing various measures to counter DDoS attacks, detect and block phishing websites, and handle other threats.

In addition, we periodically conduct risk analysis using cybersecurity heat maps and third-party assessments using international cybersecurity assessment tools such as FFIAC-CAT*2. We also participate in cyber exercises organized by the Financial ISAC*3 and the Cabinet Cybersecurity Center, running through the PDCA cycle to enhance our countermeasures and cyber resilience. Furthermore, we are also prepared for emergencies through our cyber insurance.

(5) Responding to the New Normal

In response to the COVID-19 pandemic, work from home and telework environments are rapidly expanding in the Group. For cybersecurity risks related to teleworking, we implement thorough security measures and information management for remote terminals and other equipment, and confirm safety through risk assessments and penetration tests.

(6) Security Personnel Development

To develop personnel with advanced expertise in cybersecurity, CSIRT collaborates with external experts in internal review meetings, participates in external communities such as Financial ISAC and FS-ISAC*4, provides external training and certification support, and sends employees to graduate schools.

We also make ongoing efforts to educate employees through information security training for all employees, phishing e-mail drills, and cyber exercises in cooperation with external organizations.

(7) System Risk Management Framework

In order to minimize the impact of large-scale failures and disasters on our information systems and prepare for early recovery and business continuity, we are working to strengthen our resilience by specifying the Group's communication and response systems in detail, developing workarounds and recovery procedures, and conducting education and training in operations.

In addition, to address the risk of delays and cost increases resulting from system development over a certain scale, we monitor the progress and quality management of largescale system development projects and report them to the IT Committee for discussion in an effort to ensure appropriate management of system development.

(8) IT Committee

The IT Committee is composed of the Officers and general managers in charge of each business management department, including the IT System Planning and Management Department, as well as external members, and examines and discusses important system investments and system technology from a multifaceted perspective. In terms of risk management, the IT Committee shares and discusses risks arising from system development, cybersecurity, and system risks, etc., and as an advisory body to the Board of Directors, actively utilizes the knowledge of external committee members, who are experts from outside the company, to enhance discussions and improve management.

*1 CSIRT (Computer Security Incident Response Team): In-house organization that collects, analyzes, and responds to early warning information about attacks
*2 FFIEC-CAT (Cyber Security Assessment Tool): A cybersecurity risk assessment tool published by FFIEC (Federal Financial Institutions Examination Council) for financial institutions
*3 Financial ISAC (Information Sharing and Analysis Center): Information sharing organization for Japanese financial institutions
*4 FS-ISAC (Financial Services Information Sharing and Analysis Center): Information sharing organization for financial institutions, mainly in the United States

7 Crisis Management

The Group has developed systems to swiftly and appropriately implement emergency and crisis response measures in the event of natural disasters, computer system failures, outbreaks of new infectious diseases, and the like, which are rooted in its public mission and social responsibilities as a financial institution, and strives to disseminate information regarding these systems throughout the organization.

Specifically, we have developed BCPs (business continuity plans) for continuing business in the event of a crisis, after securing the safety of our clients, directors, officers, employees, and their families. In order to ensure the effectiveness of our BCPs, we periodically conduct exercises and revise their content.

In addition, we have created a response system in which, in the event of a crisis, an emergency response headquarters is created, which is headed by the President. For natural disasters such as large earthquakes and large-scale wind and flood disasters, which are envisioned as having a significant impact, we are enhancing our response system through the preparation of backup offices and backup systems.

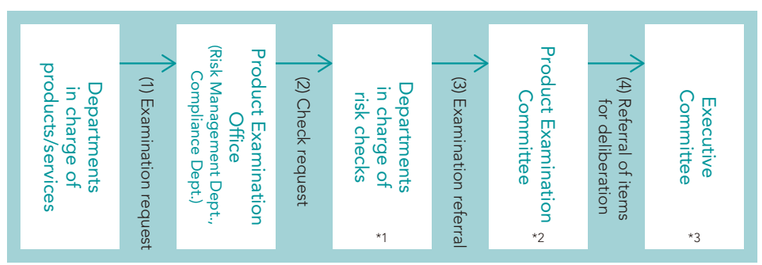
To address risks related to business continuity amid the COVID-19 pandemic, we established an emergency task force and set our basic stance of "ensuring the health and safety of our employees and their families," "maintaining business continuity as a key piece of social infrastructure," and "preventing the spread of infection in population (including activities that make the population less vulnerable)." In accordance to our stance, we have flexibly implemented measures while taking into account the COVID-19 infection situation in Japan and overseas, government requests, client trends, etc. In addition, we have implemented various business continuity measures as stipulated in our BCP and actively utilize teleworking in order to balance the maintenance of services with safety considerations.

8 New Product and Service Examination System and Post-Introduction Management System

When introducing a new product or service, it is necessary to develop various systems in order to continue offering the product or running the operation, including making an advance determination regarding the existence of any inherent risks and identifying their types, evaluating and managing such risks, and providing explanatory materials and methods to clients. To that end, we have developed a new product and service examination system. In the examination process, multiple departments carry out verification from various angles, with an emphasis on introducing products and services that will earn the trust of clients.

For products and services that have been examined by the Product Examination Committee, after they are introduced, we regularly monitor the status of our post-introduction initiatives, including from a risk management perspective. Regular monitoring is also carried out from the viewpoint of providing clients with appropriate explanations for products and services that are expected to be affected due to changes in the environment and so on, regardless of whether or not they have been deliberated by the Product Examination Committee. The results of these verifications are reported to the Product Examination Committee, and in the event that a situation arises that differs from the assumptions at the time of review, we discuss how to address and report the details to the officers in charge of the Risk Management Department and the Compliance Department.

■Product Examination Process (SuMi TRUST Bank)



*1 Risk Management Dept., Compliance Dept., Legal Dept., Planning and Coordination Dept., Fiduciary Duties & Customer Satisfaction Planning and Promotion Dept., Financial Planning Dept., Business Process Management Dept., etc.
*2 Held jointly with the Conflicts of Interest Management Enhancement Committee as necessary to consider merchantability and the perspective of conflicts of interest.
*3 When new products and services that may have a significant impact on the Group's management are referred to SuMi TRUST Bank's Executive Committee, discussions are held with SuMi TRUST Holdings, and a framework is provided for bringing up matters at the Executive Committee and reporting to the Board of Directors.