

# Risk Management

## 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 risk management framework of the Group incorporates a Risk Appetite Framework\*. It functions organically within the Group in an interconnected manner.

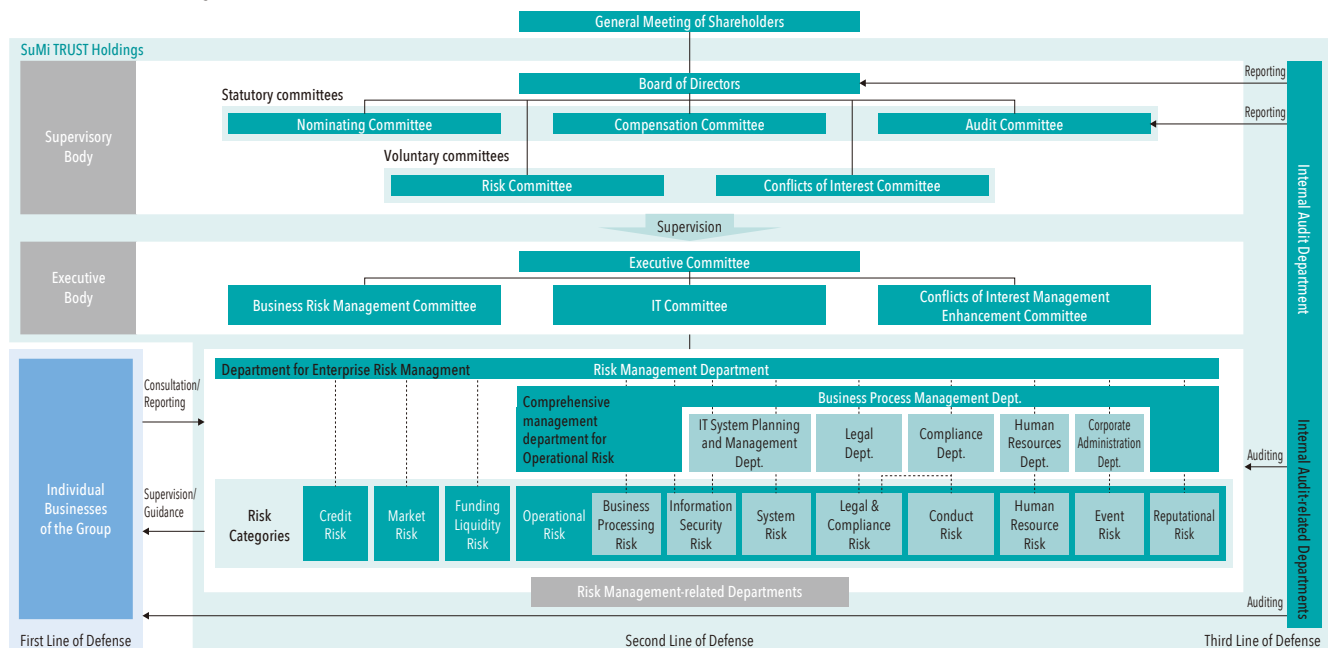
\*The Risk Appetite Framework (RAF) is a group-wide corporate management framework consisting of the process for determining risk appetite (the type and amount of risk to be willingly taken to achieve the management plan) within the Group's risk capacity, in order to achieve management strategies formulated 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.

## 2. 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. Businesses take risks within the scope of the risk appetite based on established risk-taking policies. They evaluate the risks, and if a risk falling outside the scope of the risk appetite materializes, risk control is implemented swiftly at the operational level. 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.

## Risk Management

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 verifies 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.

## 3. 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 Analysis, Evaluation, and Measurement

For the risks that are identified as subject to management, we conduct appropriate risk analysis, evaluation, and measurement that align with the scale, characteristics, and risk profiles of the Group's businesses. Among these, with regard to "significant risks," periodic evaluations are conducted to measure frequency, impact, and severity. Decisions are then made about whether they qualify as top risks (risks that require management attention due to their potential to have a significant impact on the Group's ability to conduct business or on its performance objectives within the year) or emerging risks (risks with the potential to have a significant impact in the medium to long term, over a year from now).

### (3) Risk Monitoring

Risk conditions are monitored at an appropriate frequency while taking into consideration the internal environment of the Group (risk profiles, usage of allocated capital, etc.) and the external environment (economy, markets, etc.), with KRI\* and other indicators being set. Recommendations, guidance, and advice are provided to the Group's businesses as required.

The details of the monitoring activities are reported and submitted to the Board of Directors, Executive Committee, and other bodies periodically, or on an as-needed basis.

\*KRI: Key Risk Indicator

### (4) Risk Control and Mitigation

When events that could have a significant impact on the soundness of management occur, such as the amount of risk exceeding the risk appetite's allowable range or risk limit, or when there is a fear that such limits might be exceeded, reports are made as appropriate to the Board of Directors, the Executive Committee, and other bodies, and necessary measures are taken in accordance with the severity of the risk.

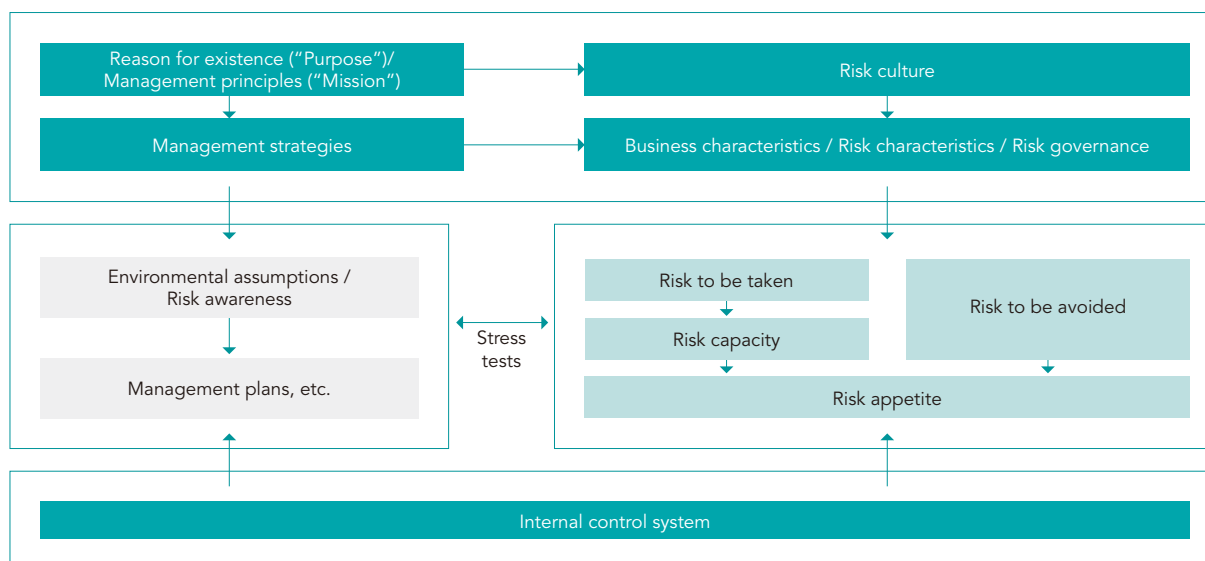
## 4. Risk Appetite

### (1) Outline of the Risk Appetite Framework

The Risk Appetite Framework 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 decisionmaking 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 group 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

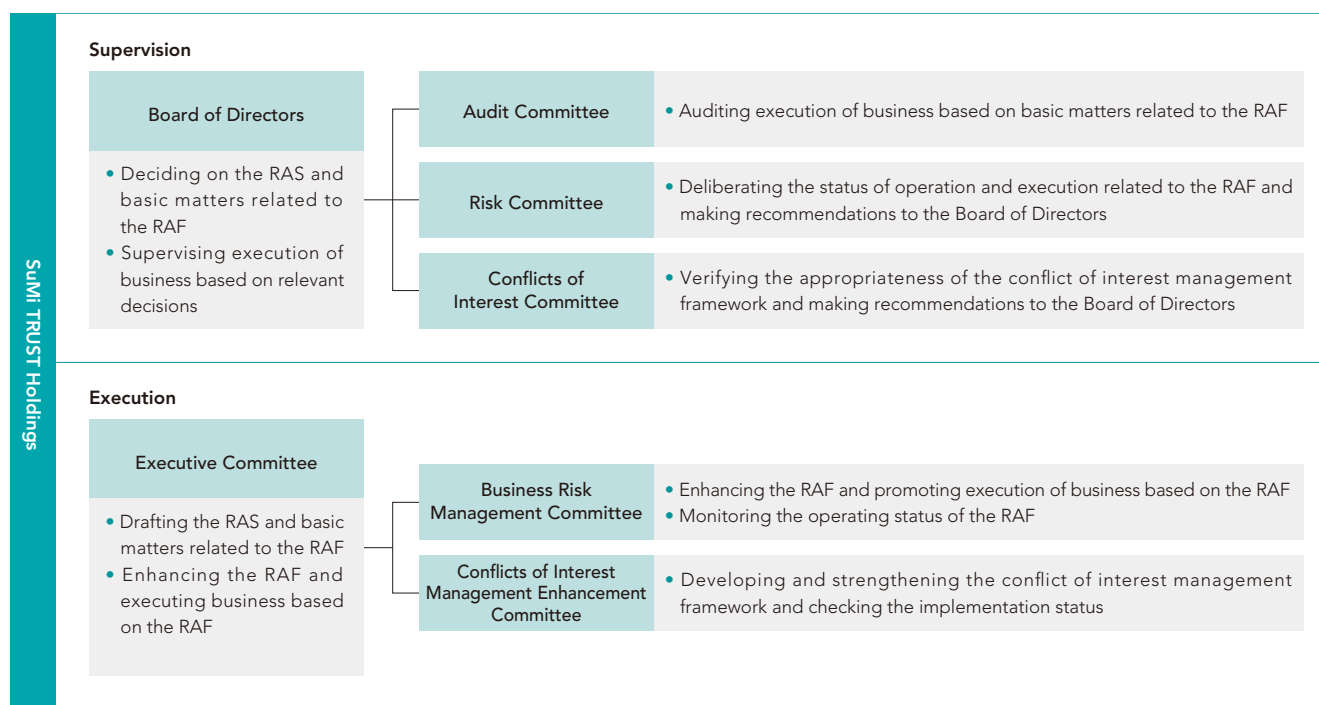
based on its business model, the Group sets separate risk appetite indicators from the three perspectives of return, risk, and cost, and monitors them regularly. If the indicators deviate from the set levels, the Group analyzes the cause and implements countermeasures or reconsiders the levels of risk 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 Management

### Risk Appetite Framework Management System



## 5. The Group's Risk Characteristics

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

In addition, SuMi TRUST Bank regularly assesses the status of major conduct risks and strives to reduce and manage risks and prevent risks from materializing by instilling and fostering awareness among executives and employees through internal training and other means.

From a forward-looking perspective, the Group's top management regularly identifies top risks and emerging risks, monitors and controls these risks, implements countermeasures, and reports to the Board of Directors

and other relevant parties. The Group's main top and emerging risks related to sustainability and the countermeasures taken to address them are listed below.

### Risks related to the global COVID-19 pandemic [Risk Details]

The global spread of COVID-19, if it becomes long-term, could have a negative impact on the world economy. For the Group, the quality of its credit portfolio may deteriorate, credit-related costs may increase, and adverse effects on business strategy might arise due to negative impacts on obligor businesses. In addition, if infections increase among Group employees and related parties, there is a possibility that business continuity may be compromised. These issues could have a negative impact on the Group's business operations and performance.

### [Countermeasures]

The Group conducts periodic stress tests of its credit portfolio based on macroeconomic scenarios and formulates action plans in preparation for times of stress. With regard to the risks associated with loan-related costs, based on the economic environment and the fluctuation of internal ratings, etc., assumptions were made about the degree of future credit risk deterioration by industry and internal rating in accordance with the degree of impact on performance due to the spread of COVID-19 and the extent of

the prospects of recovery after the pandemic's end. An estimate was then made of the credit loss expected to occur in the future for a portion of loans in the industry, and an additional allowance for doubtful accounts (special allowance) have been provided.

With regard to the risks associated with business continuity, an emergency headquarters has been established on the following basic stances: ensuring the health and safety of employees and their families, ensuring business continuity as a key piece of social infrastructure, and preventing the spread of infection in society (including activities aimed at forming a society that is less likely to spread infection). We have been making flexible responses based on the infection situation domestically and overseas, government requests, customer trends, and other factors, and are trying to balance service maintenance and safety by implementing a variety of business continuity measures defined as crisis management and business continuity (BCP) in the event of disasters, as well as active utilization of telework and so on.

### Risks related to cyberattacks

(See pages 47-49 for details)

### Legal & compliance risk

#### [Risk Details]

The Group strictly complies with the Banking Act, the Financial Instruments and Exchange Act, the Act on Engagement in Trust Business by a Financial Institution, and other laws and regulations. However, any failure by executives and employees to comply with these laws and regulations could result in penalties or administrative action against the Group, or loss of reputation in the market. In addition, there is a possibility that the products and services provided by the Group may not meet client expectations, and that the Group may be sued for damages due to various problems and claims that arise in the course of conducting its business. These factors could adversely affect the Group's business operations, performance, and financial condition.

#### [Countermeasures]

The Group has formulated a compliance program and manages the state of progress and achievement of the program in order to maintain an appropriate compliance framework in line with the characteristics of each of the Group's businesses.

The Group is improving training on compliance throughout the entire Group to help foster an awareness of compliance matters. Specifically, we provide training materials used in e-learning programs and discussion-based study sessions to Group companies on themes that span the whole Group.

Each Group company conducts training and study sessions tailored to the characteristics of business and products at each company and the aspects of their clients, as well as e-learning programs on specific themes.

### Risks related to data management

#### [Risk Details]

The Group manages client data and basic data necessary for business management (hereinafter referred to as "management information, etc.") through various systems, to provide a number of services to clients and for external reporting, etc.

In terms of handling management information, etc., the challenges are the expansion and enhancement of the scope of business to which the data governance system established in line with the "Principles for effective risk data aggregation and risk reporting" (BCBS 239) of the Basel Committee on Banking Supervision is applied, as well as the operation of an effective quality control framework for important reports.

Deficiencies in these data quality management processes for management information, etc., could lead to errors in management decision-making and not only lower the Group's corporate value and result in a loss of trust, but also have a negative impact on business operations and performance.

#### [Countermeasures]

The Group has established a control framework for the management of personal information and management information, etc., and is striving to continuously strengthen data management, as well as upgrade data governance in line with BCBS 239.

Every fiscal year, we formulate an MIS Plan (a resource allocation plan for improving the effectiveness of the Management Information System) and a Data Control Environment/Maintenance Improvement Plan. These plans aim to enhance our Management Information System and improve the quality of our reporting and data through the PDCA cycle of our Quality Management Framework for important reports.

We establish policies and procedures for information management, and we educate and train our staff thoroughly to ensure they understand its importance.

### Risks related to climate change

#### [Risk Details]

Medium- to long-term climate change could potentially have a negative impact on the Group's performance and financial condition owing to greater risk of physical damage to, for example, the natural environment, social infrastructure, and client assets (physical risks), as well as the risk of a rapid transition to a low-carbon society owing

## Risk Management

mainly to policy changes, changes in social norms, financial market preferences regarding climate change, and technological innovation (transition risks).

Specifically, we recognize that there are physical risks such as the deterioration in the credit status of our obligors and the value of pledged assets due to natural disasters, as well as transition risks such as the potential for a decline in the prices of assets held by the Group, such as securities issued by companies that emit a large amount of carbon dioxide and corporate credit loans offered to such companies, resulting from the rapid transition to a low-carbon society.

### [Countermeasures]

The Group, based on the final recommendations of the Task Force on Climate-related Financial Disclosures (TCFD) of the Financial Stability Board (FSB) in June 2017, manages climate change-related risks within its Group-wide risk management framework.

In terms of credit risk management, we formulate sector-specific policies, and in principle prohibit new loans from going to coal-fired power plants that emit a large amount of greenhouse gases. We also periodically monitor related indicators.

From a medium- to long-term perspective, we conduct simulations to measure the impact that transition and physical risks may have on the Group.

For more details, refer to the separately issued TCFD report (Chapter 2: Strategy, Chapter 3: Risk Management).

 <https://www.smth.jp/english/-/media/th/english/sustainability/report/2022/TCFD-E-all.pdf>

### Emerging Geopolitical Risks (Crisis in Ukraine, etc.)

#### [Risk Details]

The direct impact on the Group due to the prolonged Russia-Ukraine conflict is limited. However, if the conflict were to negatively impact the global economy, it could indirectly harm the Group by affecting the businesses of its obligors, increasing loan-related costs due to a deterioration in the quality of the credit portfolio, and negatively influencing our business strategy. In addition, international sanctions could disrupt some of our international operations. These issues could have a negative impact on the Group's performance.

#### [Countermeasures]

The Group regularly conducts stress tests based on macroeconomic scenarios for its credit portfolio and formulates action plans for periods of stress. The stress tests include simulations of rising resource prices due to the Russia-Ukraine conflict and estimate their impact on the Group's performance.

As for the impact on the Group's business operations, we monitor changes in the situation in Ukraine and respond in a flexible manner that takes government requests and customer trends into consideration.

### Risks related to innovation

#### [Risk Details]

The advancement of fintech and other technologies related to the financial business is progressing beyond the boundaries of the industry and changing the behavior of clients. If the Group is unable to adapt to these changes, our competitiveness may decline or the scale of our business may shrink, which may adversely affect our business performance and financial condition.

#### [Countermeasures]

We will work to improve the efficiency of existing business operations by utilizing digital technology and create new platforms in areas unique to trust banks.

### Risks related to Japan's declining birthrate and aging population

#### [Risk Details]

The demographic changes in Japan will result in changes in age composition of the Group's clients over the medium to long term. The number of clients for the Group's individual consulting and mortgage loan services may decline over the medium to long term, which may adversely affect the Group's performance and financial condition.

#### [Countermeasures]

As we enter an age of 100-year life, there is growing interest in asset formation due to concerns over retirement savings, and we are working to evolve and upgrade our business model to one unique to our Group, utilizing the diverse functions of a trust bank.



## 6. 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 (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 value against our corporate strength (capital position), 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 Group 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.

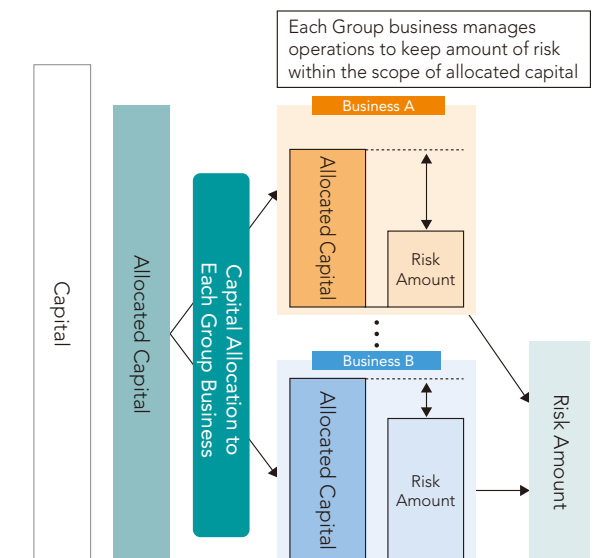
The capital allocation plan is subject to the approval of the Board of Directors. Capital allocation levels are determined based on the Group's risk appetite.

Each Group 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.

### Capital Allocation Scheme



### Hypothetical Scenario Stress Testing

We assess capital adequacy level by formulating stress scenario that has a sufficiently strong impact and a realistic probability of occurrence and then estimating capital adequacy ratio, etc. in times of stress.

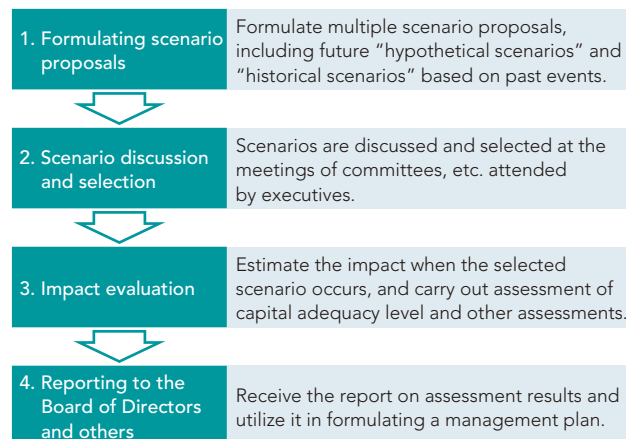
### Historical Scenario Stress Testing

We also assess capital adequacy level through estimation of capital adequacy ratio, etc. in times of stress using parameters from stress times that had occurred in the past.

### Examination of Probability of Occurrence

We further assess capital adequacy level by comparing the risk with 99.9% confidence interval with total capital defined under capital adequacy requirements.

### Stress Test Framework



### 7. 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 executives and employees, that flexibly excute 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

Group 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 clearly stating our RAF, which is used as a common language in lively discussions concerning risk appetite within the Group.

### 8. Crisis Management and Business Continuity Plan (BCP) in Disasters

#### The Group's Initiatives

The Group has developed contingency plans in order to quickly implement emergency response measures in the event of emergencies, such as natural disasters, computer system breakdowns and outbreaks of new infectious diseases.

Moreover, regarding important business operations, such as financial settlement, SuMi TRUST Holdings and SuMi TRUST Bank have developed systems to continue business, including BCPs (business continuity plans) and backup offices. In order to ensure the effectiveness of such systems, they periodically conduct exercises and revise BCPs.

When the crisis is serious and its impact is extensive, causing serious disruptions to the Group's normal business operations and making it necessary to urgently make comprehensive and high-level management judgment, the Group will establish an emergency task force as a company-wide response organization and will quickly implement emergency response measures. In particular,

in preparation for the possible occurrence of a major earthquake, SuMi TRUST Bank, which has branches across Japan, periodically conducts exercises in order to make a response that gives consideration to the safety of clients and employees and to business continuity and ensure the effectiveness of the response.

As for company-wide response, in order to enhance the effectiveness of the functions of the emergency task force, the Group is strengthening systems for information gathering and information coordination, in addition to periodically conducting exercises, and it is also promoting the enhancement of emergency response systems in the Osaka area on the assumption of a disaster in the Tokyo area.

Meanwhile, branches are striving to strengthen response capability through periodic exercises and are promoting disaster countermeasures in light of individual branches' specific circumstances such as the location condition and the status of principal facilities. Branches are also developing a system for mutual support among them.

#### Code of Conduct for Executives and Employees

1. In preparation for emergencies, executives and employees are to take preventative and mitigation measures. They are to implement risk reduction measures to the extent possible to prevent adverse effects on business operations.
2. In the event of an emergency, executives and employees must make judgements and take actions based on the following principles:

##### (1) Securing the Safety of Life and Physical Health

In the event of an emergency, the top priority must be placed on securing the safety of clients, executives, employees, their families, and other stakeholders. Furthermore, during emergency responses, humanitarian considerations shall always take priority.

##### (2) Ensuring Business Continuity and Early Recovery as a Key Piece of Social Infrastructure

In the event of an emergency, considering the role of SuMi TRUST Bank and the Group as a key piece of social infrastructure, executives and employees must strive for the early recovery and continuity of priority operations in accordance with their level of importance.

##### (3) Cooperation with Local Communities

In the event of an emergency, executives and employees must strive to cooperate with local communities, which includes offering assistance and support for life-saving and emergency activities in the area.

##### (4) Protection of Corporate Assets

In the event of an emergency, executives and employees must aim to preserve the corporate assets of the Group.



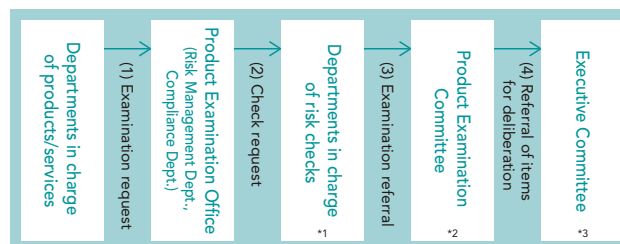
## 9. New Product and Service Examination System and Post-Introduction Management System

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.

### 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.

## 10. Information Security Risks and Cybersecurity Measures

### Information Security Risk Management Framework

The 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 governance and management framework materiality. 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.

### Regulations related to information security risk management

Regulations	Declaration of the Protection of Personal Information, Risk Management Regulations
Rules	Risk Management Rules, Operational Risk Management Rules, Information Security Risk Management Rules, System Risk Management Rules
Guidelines	Information Security Risk Management Guidelines, System Risk Management Guidelines, Personal Information Handling Guidelines, Personal Data Administrative Guidelines, CSIRT Operational Guidelines, Internal OA Management Guidelines, Administrative Guidelines for Taking Client Information Outside the Company, etc.

### 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

## Risk 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.

<b>Organizational structure</b>	Board of Directors, Executive Committee Business Risk Management Committee (SuMi TRUST Holdings) Operational Risk Management Committee (SuMi TRUST Bank)
<b>Officer in charge</b>	Officer in charge of Business Process Management Department or officer in charge of IT System Planning and Management Department
<b>Control departments</b>	Business Process Management Department and IT System Planning and Management Department

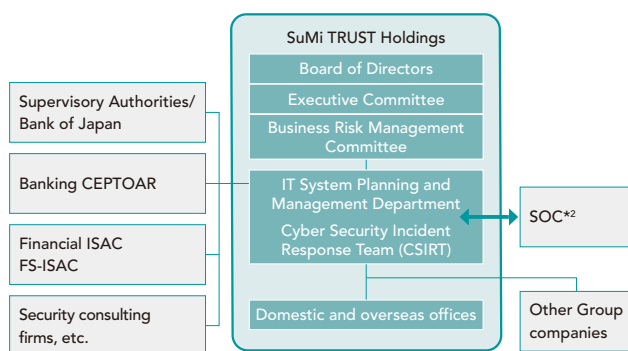
### Cybersecurity Management Framework

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 SuMiTRUST-CSIRT\*<sup>1</sup> 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.

### Cybersecurity Management System



\*1 CSIRT (Computer Security Incident Response Team): In-house organization that collects, analyzes, and responds to early warning information about attacks

\*2 SOC: Abbreviation for Security Operation Center. The SOC monitors networks to detect and analyzes cyberattacks.

In addition to conducting cybersecurity risk assessments and system vulnerability assessments on a regular basis for the 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.

### 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, and we have established a monitoring system centered on the CSIRT.

### 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 FFIEC-CAT\*<sup>2</sup>. We also participate in cyber exercises organized by the Financial ISAC\*<sup>3</sup> 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.

Key technical measures	
<b>Entry measures</b>	<ul style="list-style-type: none"> <li>Detect and block malicious traffic (including countermeasures to DDoS)</li> <li>Stop viruses and malware (suspicious applications) from intruding</li> </ul>
<b>Exit measures</b>	<ul style="list-style-type: none"> <li>Restrict suspicious traffic through behavior detection</li> <li>Assess and enhance the internet route through vulnerability assessment through vulnerability assessment</li> </ul>
<b>Internal measures</b>	<ul style="list-style-type: none"> <li>Detect of malware behavior that has infiltrated endpoints (internal office automation terminals and servers)</li> </ul>
<b>Integrated monitoring</b>	<ul style="list-style-type: none"> <li>Improve detection accuracy through integrated analysis of multiple access logs obtained from firewalls, proxy servers, etc.</li> <li>Expand scope of detection by decrypting encrypted communications (e.g., HTTPS) before analysis</li> </ul>

\*1 FFIEC-CAT (Cyber Security Assessment Tool): A cybersecurity risk assessment tool published by FFIEC (Federal Financial Institutions Examination Council) for financial institutions

\*2 Financial ISAC (Information Sharing and Analysis Center): Information sharing organization for Japanese financial institutions

### 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.

### 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\*, 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.

\* FS-ISAC (Financial Services Information Sharing and Analysis Center): Information sharing organization for financial institutions, mainly in the United States

### 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 large-scale system development projects and report them to the IT Committee for discussion in an effort to ensure appropriate management of system development.

### 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.

#### IT-related Risk Governance Structure

