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

2. 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.

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.

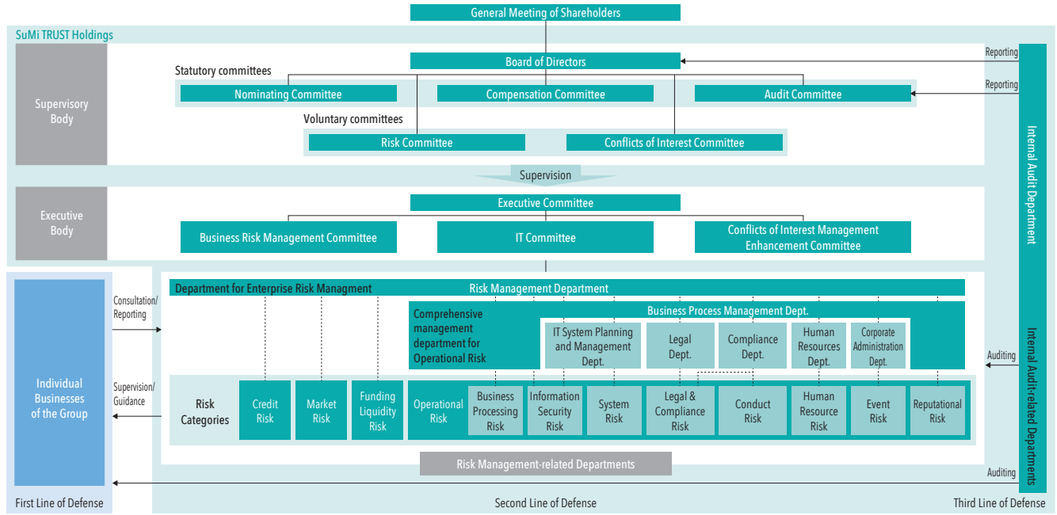
■Risk Definition

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.

3. 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 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 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.

4. 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

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.

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 are selected, and risk predictors are monitored. Countermeasures are implemented based on the monitoring results for both types of risks.

The top risks at present include "the global COVID-19 pandemic" and other risks. Along with countermeasures, these risks are reported to the Board of Directors and the Executive Committee. Emerging risks at present include "climate change" and other risks, and we are analyzing these risks and considering necessary countermeasures.

The Group's main top risks and emerging risks are listed in the table below.

■ Main top risks and emerging risks

Top risks	Risks related to the global COVID-19 pandemic
	Risks related to falling prices for strategic shareholdings and similar assets
	Risk of concentration of credit in major obligors in the credit portfolio
	Risks related to cyberattacks
Emerging risks	Risks related to climate change*
	Risks related to innovation
	Risks related to Japan's declining birthrate and aging population

* The Group is taking steps to enhance the sophistication of its management of climate change-related risks, for example by identifying major climate-related risks in its portfolio and conducting scenario analyses.
For more information, please refer to our TCFD Report published in December 2020.

(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.

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 (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 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. Cyber Security and Systems Maintenance

Based on the selection of cyberattacks as a top risk, The Group has formulated its Cyber Security Management Declaration against cyberattacks, and is working to strengthen security measures led by management. Specifically, SuMi TRUST Holdings has established SuMiTRUST-CSIRT*1 as an internal management system that collects and analyzes threat and vulnerability information from both inside and outside the group, develops necessary security measures, deploys them, and reports them to top management on a regular basis. We share and utilize the latest cyberattack techniques and vulnerability information using CSIRT as well also other information sharing organizations such as Financial ISAC*2 and FS-ISAC*3, and conduct cyber security exercises on a regular basis to strengthen our ability to respond to cyberattacks. In addition, we are working to strengthen and standardize security measures Group-wide by deploying common security measures such as a common Internet infrastructure and SOC*4 monitoring, as well as by promoting Group-wide standardization of security assessments using international assessment tools such as FFIEC-CAT*5. With respect to systems maintenance, 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.

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

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 large-scale natural disasters such as earthquakes, 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.