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 financial group specialized in trust banking, 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's businesses consist of the Retail Total Solution (TS) Services Business, the Wholesale Total Solution (TS) Services Business, the Wholesale Asset Management (AM) Business, the Stock Transfer Agency Services Business, the Real Estate Business, the Global Markets Business, and the Fiduciary Services Business, etc.

The Group faces various risks, including credit risk, market risk, funding liquidity risk, and operational risk,

Businesses and Main Risk Characteristics of the Group

Risk Category / Individual Businesses	Retail TS	Wholesale TS	Wholesale AM	Stock Transfer Agency Services	Real Estate	Global Markets	Fiduciary Services	Asset Management	Corporate Management*
Credit Risk	○	○	○			○			
Market Risk		○				○			○
Funding Liquidity Risk						○			
Operational Risk	○	○	○	○	○	○	○	○	○

* Strategic shareholdings management, etc.

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 country of obligors.
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 the Group may incur losses due to inadequate or failed bussiness 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.
	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.

which vary depending on the business characteristics of each of the Group's businesses. With regard to trust business risks, SuMi TRUST Bank provides management primarily 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.

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).

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 engages in risk taking within the established range of risk appetite, and, when a risk materializes, promptly implements risk control at the on-site level.

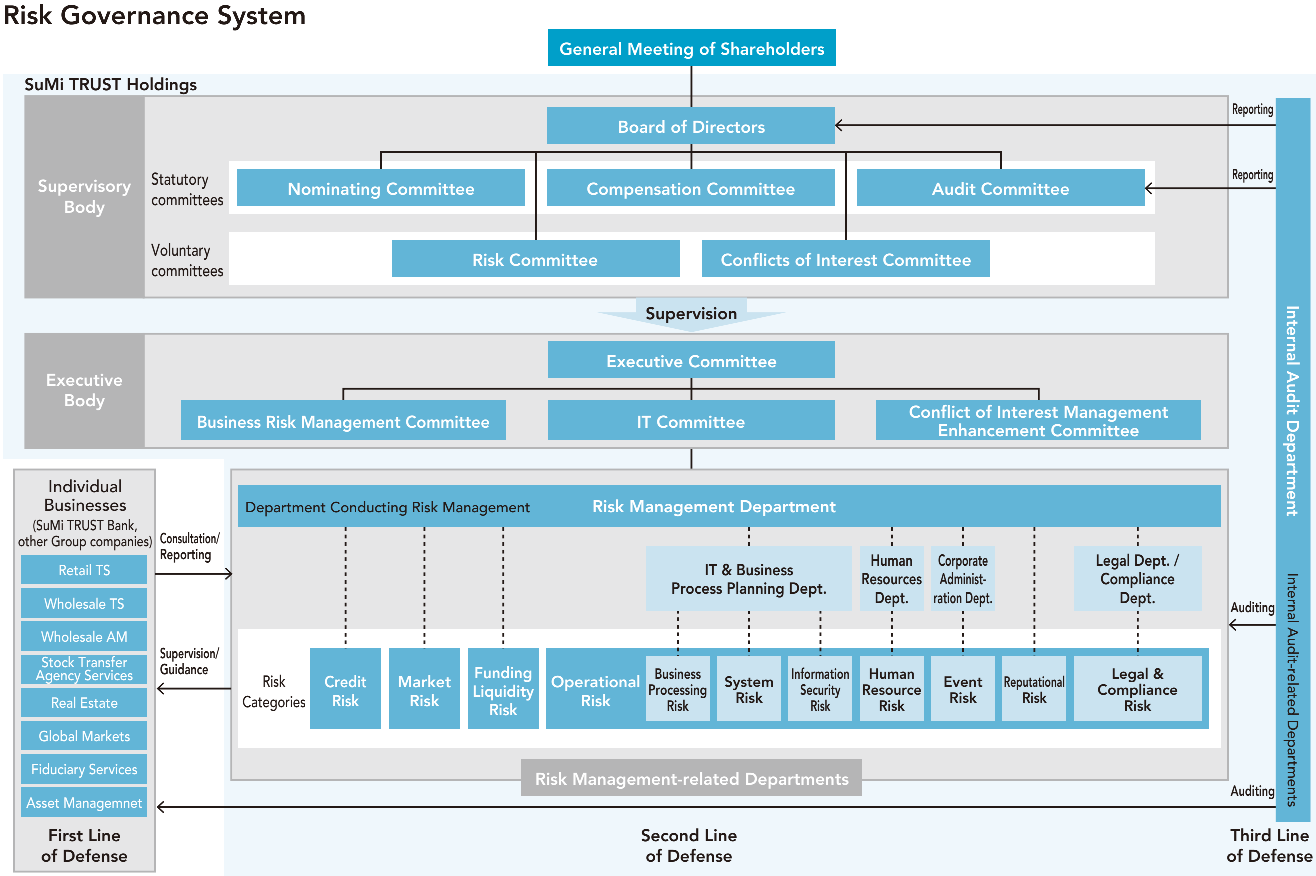
Second Line of Defense

The 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.

The Risk Management Department and risk management-related departments act as a restraint function for the risk taking of the first line of defense, and supervise and provide guidance regarding the risk governance system.

The Risk Management Department reports on the status of risk management to the Executive Committee and the Board of Directors.

Risk Governance System



Third Line of Defense

The Internal Audit Department verifies the effectiveness and appropriateness of the group-wide risk governance system and processes from an independent standpoint.

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.

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.

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.

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.

When risks cannot be quantified, their impact is assessed to the greatest extent possible, and they are managed through measures such as implementing preventive measures based on the nature of the risks.

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 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 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.

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 (risks that have a high probability of occurrence and that would have a large impact on the Group) are selected, and risk predictors are monitored. Countermeasures are implemented based on the monitoring results for all types of risks.

Our top credit risks include "worsening of credit among major obligors," our top market risks include "falling prices for strategic shareholdings, etc.," and our top operational risks include "cyber-attacks."

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).

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).

(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.

Stress Tests with Hypothetical Scenarios

We assess capital adequacy level by formulating plausible stress scenarios that are sufficiently strong and realistic to estimate capital adequacy ratio during times of stress.

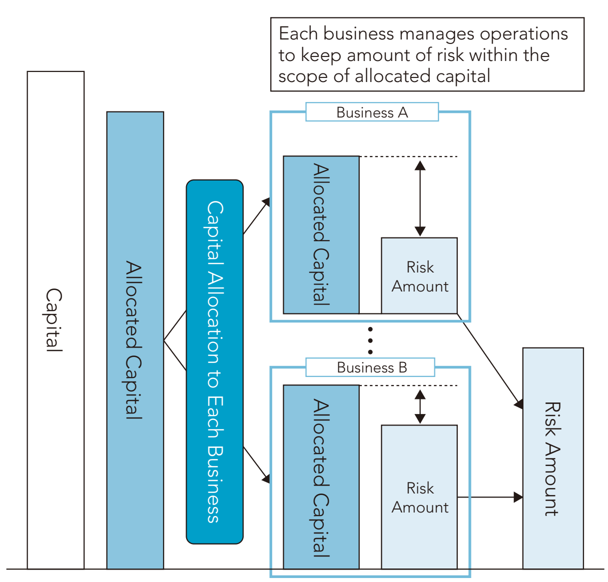
Stress Tests with Historical Scenarios

We also assess capital adequacy level by using parameters from previous times of stress to estimate capital adequacy ratio during times of stress.

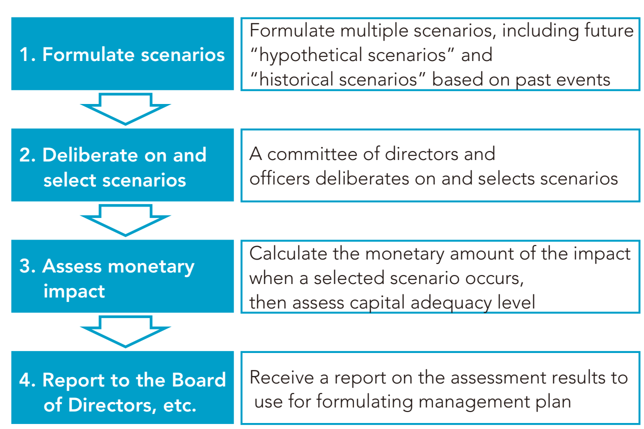
Likelihood Validation

We further assess capital adequacy level by calculating the amount of risk (with a confidence interval of 99.9%) to compare those figures with total capital under capital adequacy regulations.

Capital Allocation Scheme



Stress Test Framework



6. Managing Risk in Each Risk Category

(1) Managing Credit Risk

1) Definition of Credit Risk

Credit risk is "risk that the Group incurs losses due to the value of an asset (including off-balance sheet assets) decreasing or impairing owing to such reasons as deterioration in the financial condition of an obligor." Of this, country risk in particular means "risk that the Group incurs losses on credit provided overseas, due to foreign exchange, political, and economic conditions of the country of the obligor."

2) Characteristics of Credit Risk

Credit risk is the most fundamental risk related to "credit creation," the primary function of a finance. As the Group manages bank operations, it is also an important risk affecting the Group.

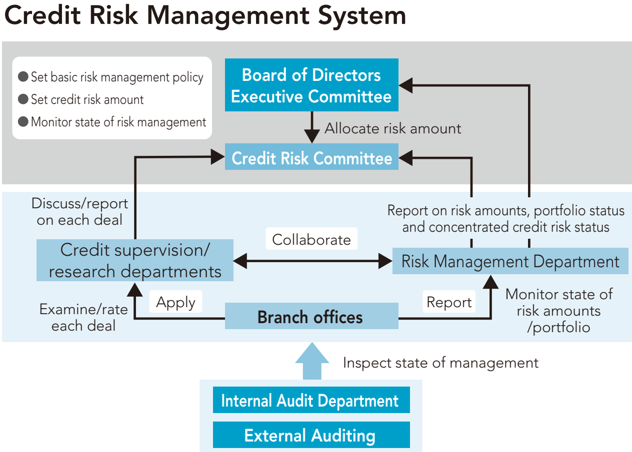
The major credit risk affecting the Group is the risk of sizable bad debt (or the provision of reserves) due to a default or deteriorated credit for a large obligor. To properly control for "concentrated credit risk" arising as the result of concentrated credit at a certain company or company group and "the risk of default chain" reaction arising as the result of concentrated credit to a region or industry, the Group sets credit guideline amounts according to borrower ratings and country ratings and conducts monitoring of loan balances and risk amounts in each industry.

3) Credit Risk Management Policy

The Group's basic policy on credit risk management consists of two parts: "strict management of individual loans" and "a decentralized credit portfolio." The first is a meticulous process of managing individual loans by screening and studying deals, self-assessment, internally assigned credit ratings and so forth. The latter involves efforts to mitigate concentrated risk by managing the decentralization of the overall credit portfolio, including large accounts, by industry and country. In addition, we measure credit risk amounts to quantitatively understand the portfolio's potential for loss.

Furthermore, to set "appropriate risk-return," we configure earnings levels that include such factors as anticipated losses and expenses for each credit rating, and we strive to ensure a certain profit margin (i.e. spread) proportionate to the risk by reflecting the terms of each deal.

Credit Risk Management System



4) Credit Risk Management System

The Bank supervises group-wide credit risk management while endeavoring to build structures for each group company. SuMi TRUST Bank has built a structure for managing consolidated and global based risk while managing credit risk.

5) Credit Risk Management Method

The Group takes two mutually complementary approaches to properly manage credit risk in our efforts to construct and sustain a sound portfolio. The first is "management of individual loans," which is done through inspection of new loans and management during the term of a loan. The other approach is "credit portfolio management," by which we analyze and assess factors such as the state of concentrated risk to particular industries, regions, or company groups via statistical techniques to gain an understanding of all loans as a single portfolio, then manage from a macro perspective.

(2) Managing Market Risk

1) Definition of Market Risk

Market risk is "risk that the Group incurs 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." Of this, market liquidity risk in particular means "risk that the Group incurs losses caused in a situation where it becomes impossible to conduct transactions in the market or becomes obligatory to trade at prices much more disadvantageous than usual due to market turmoil, etc." In addition, there is interest rate risk in the banking book (IRRBB), which is risk of harm to a bank's capital or profit/loss, either in the present or future, due to interest rates fluctuating to the disadvantage of banking book positions.

2) Characteristics of Market Risk

SuMi TRUST Bank engages in banking operations to ensure earnings through interest rate risk control on assets and liabilities, while also engaging in trading operations to ensure earnings from transactions such as short-term buying and selling to leverage interest rates and foreign exchange rates. We manage market risk by using VaR and other methods in both types of operations. In trading, we seek to secure steady earnings through market-making operations in foreign exchange rates, derivatives and the like.

The major market risk affecting the Group is the risk of losses from price declines in held assets such as strategic shareholdings. The basic policy for the strategic shareholdings held by SuMi TRUST Bank is to reduce balances while we endeavor to properly control risks through hedging and other means.

Additionally, IRRBB may arise in banking book positions due to a maturity mismatch (gap risk), interest rate mismatch (basis risk), optionality accompanying interest rate changes (optionality risk) or the like. Interest rate risks at SuMi TRUST Holdings and SuMi TRUST Bank are low.

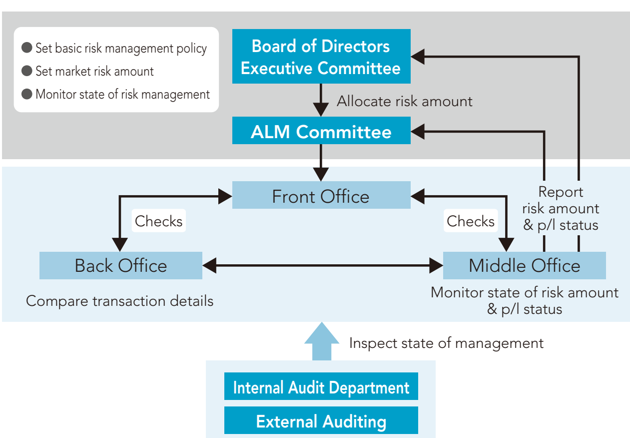
3) Market Risk Management Policy

To manage market risk, we seek to guarantee sound operations by properly controlling the risk, while we work to develop more sophisticated management systems, thus ensuring proper earnings in line with the Group's strategic targets as well as the scale and characteristics of our business. Furthermore, when controlling for interest rate risk, we hedge through interest rate swaps and other means, while applying hedge accounting to transactions that fulfill the requirements for doing so.

4) Market Risk Management System

The Bank supervises group-wide market and funding liquidity risk management while endeavoring to build structures for each group company. SuMi TRUST Bank has built a structure for managing consolidated and global based risk while managing market and funding liquidity risk.

Market Risk and Funding Liquidity Risk Management System



5) Market Risk Management Method

The Bank formulates capital allocation plans to allocate capital to group companies within the amount of capital available. SuMi TRUST Bank sets limits based on allocated capital and also sets loss limits, thereby managing to keep amounts of risk and losses within a certain range.

In addition, for interest rate risks we set alarm points to monitor changes in the economic value of positions.

(3) Managing Funding Liquidity Risk

1) Definition of Funding Liquidity Risk

Funding liquidity risk is "risk that the Group incurs 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."

2) Characteristics of Funding Liquidity Risk

The major funding liquidity risk affecting the Group is an intensified risk pertaining to the procurement of foreign currency if credit ratings for Japan or for Japan's financial institutions are lowered. SuMi TRUST Bank formulates medium- to long-term procurement policies tailored to the characteristics of each currency, such as market liquidity and the state of assets and liabilities, to manage stable foreign currency liquidity that can withstand market tumult and financial outflows like those that have occurred in the past.

3) Funding Liquidity Risk Management Policy

In the course of managing funding liquidity risk, our basic policy is to execute proper funding liquidity risk management based on two principles, as we have a thorough understanding that, when a risk manifests itself, the threat could directly ruin the Group's business. One of the two principles is "to seek a balance between procurement costs and stability" by various means of procurement. The other is "to prepare for emergencies" by examining procurement capabilities in a stressed environment and reviewing countermeasures in advance.

We are continuously enhancing our funding liquidity risk management system by adapting to Basel III and other international standards pertaining to bank capital and liquidity.

4) Funding Liquidity Risk Management System

Our funding liquidity risk management system operates under the same framework as the "market risk management system."

5) Funding Liquidity Risk Management Method

Limits on funding liquidity mismatches for the entire group, individual offices, and each currency act as indicators for funding liquidity risk management. We pre-define our response to when a limit is reached and conduct daily monitoring on the state of compliance. In addition, we perform stress tests for multiple scenarios, including dramatic changes in the market environment and changes in the procurement environment specific to the Group, so that we understand the amount of funds we must procure when a funding liquidity risk arises.

(4) Operational Risk Management

1) Definition of Operational Risk

Operational risk is "risk that the Group incurs losses resulting from an inadequate operational process, action of a director, officer, or employee, or system, or from an external event." The Group manages the risk by separating it into the following categories: business processing risk, system risk, information security risk, legal/compliance risk, human resource risk, event risk, and reputational risk.

2) Characteristics of Operational Risk

One of the major operational risks to the Group is impaired business operations caused by a cyberattack (ransomware or a DDoS attack*), followed by the attackers stealing and publicly releasing client information or other data belonging to the Group. By ensuring the safety of information systems, the Group takes countermeasures to prevent unauthorized access or use via cyberattacks.

* DDoS attack: Refers to a distributed denial-of-service attack. This is a method of forcing a service to cease functioning by using multiple machines to impose a massive computing load on targeted computers.

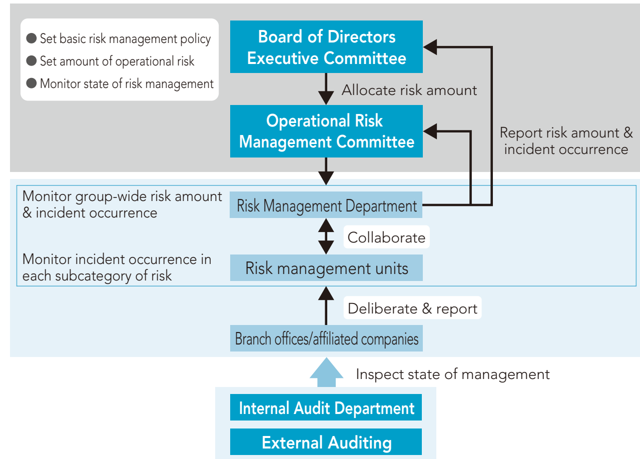
Additionally, due to inadequate measures against money laundering and terrorist financing, there are risks which include administrative penalties such as business suspension orders, payments of very large fines, and a tarnishing of the Group's reputation. The Group promotes improvements to measures for eliminating money laundering, etc. based on a gap analysis with the regulations (including overseas regulations) and a clarification of the issues involved, limits and controls risks using a risk-based approach.

3) Operational Risk Management Policy

When building the operational risk management system, the Group recognizes that some operational risk will inevitably accompany business operations. Therefore, our basic policy is to properly manage risk according to the scale and nature of the operations and particular risk, thus working to ensure that operations are sound and proper.

The Group is further upgrading our operational risk management system in preparation for the improvement of our operations and the products and services we offer, as well as the manifestation of new risks accompanying changes in society and the business environment, such as advances in information technology and diversifying client needs.

Operational Risk Management System



4) Operational Risk Management System

The Group works hard to build systems for operational risk management at group companies in line with the basic policy on group-wide operational risk management.

SuMi TRUST Bank has created a risk management department for operational risk in general, as well as risk management units for each subcategory of operational risk. The general risk management department collaborates with each operational risk management unit to form and upgrade our operational risk management system.

5) Operational Risk Management Method

The Group works to curtail operational risk by managing operational risk in all our business operations, including those of contractors, and properly assessing and identifying risk in both qualitative and quantitative terms, while also taking preventive measures against risks and formulating response, causal analysis procedures, and measures to prevent recurrence in the event a risk does manifest itself.

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

(1) The Group's Initiatives

SuMi TRUST Holdings and SuMi TRUST Bank have 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 normal business operations of SuMi TRUST Bank and the Group and making it necessary to urgently make comprehensive and high-level management judgment, the Group will establish an emergency response headquarters 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.

Code of Conduct for Executives and Employees

1. Executives and employees must fully recognize and understand the importance of crisis management and prepare for emergencies. At the same time, they must strive to develop their knowledge in normal times so that they can quickly and appropriately respond in the event of an emergency.
2. In the event of an emergency, executives and employees must make judgments and take actions based on the following principles:

(1) Securing the safety of life

In the event of an emergency, the top priority must be placed on securing the safety of customers, executives and employees, and their families. Executives and employees must also always give priority to humanitarian considerations when taking various emergency response measures.

(2) Protection of Sumitomo Mitsui Trust Bank's Corporate Assets

By taking disaster prevention and mitigation measures in preparation for the possible occurrence of emergencies, executives and employees must protect Sumitomo Mitsui Trust Bank's corporate assets in the event of an emergency. They must also do their utmost to take risk mitigation measures to guard against adverse effects that may disrupt business activities.

(3) Business Continuity and Early Restoration

In the event of an emergency, executives and employees must strive to quickly restore and continue priority business operations.

(4) Cooperation with Local Communities

In the event of an emergency, executives and employees must strive to cooperate with local communities in rescue and other local activities.

As for company-wide response, in order to enhance the effectiveness of the functions of the emergency response headquarters, 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.

(2) Response to Threat of Cyberattack

SuMi TRUST Holdings has implemented various measures in order to protect its clients' precious assets from the ever-increasing threat of cyberattack in Japan and overseas (see page 128 for details).

8. Examination System in Introducing New Products and New Operations

When introducing new products or new operations, it is necessary to develop various systems in order to continue offering products and services, including determining in advance whether there are any inherent risks and identifying their type, evaluating and managing such risks, providing explanatory materials to clients, and determining a way to explain. To that end, we have in place a system for examining the introduction of new products and new operations. In the product examination process, multiple departments carry out verification from various angles, with emphasis on introducing products and operations that will earn the trust of clients. We also conduct verification through regular monitoring after new products or new operations have been introduced.

Product Examination Process