Risk Management

Basic Philosophy

The Sanki Engineering Group's daily risk management is undertaken by the Risk Management Committee based on the Risk Management Rules. We have also established an Enterprise Risk Management system that includes operation of the Business Continuity Management System, which safeguards the effectiveness of business continuity planning in the event of contingencies.

Risk Management Promotion System

Management Based on the Risk Management Rules

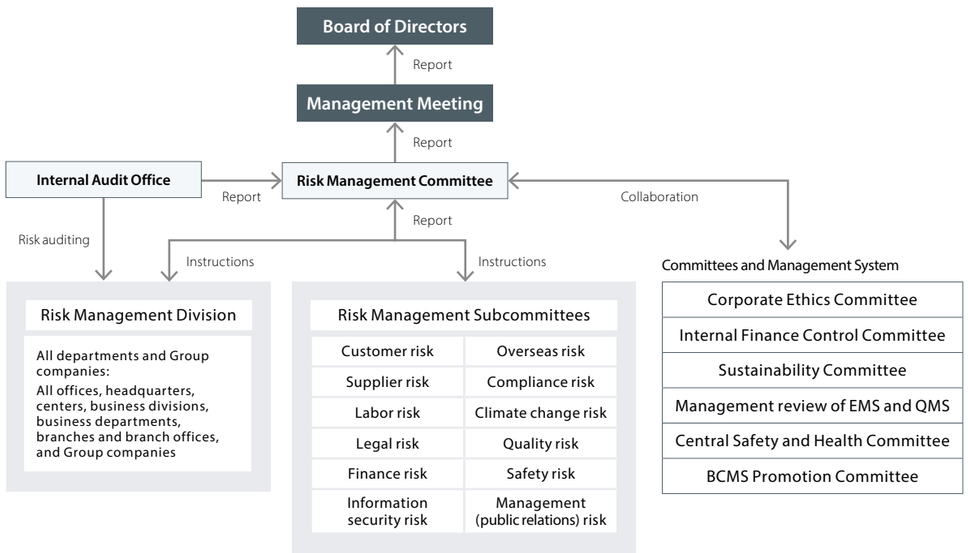
The Risk Management Committee meets quarterly, and risks are managed through the Risk Management Division and the subcommittees responsible for various risks. The Risk Management Division consists of representatives from each department and Group company and is responsible for discerning changes in the environment on a daily basis to identify emerging risk factors and managing signs of risk manifestation. The Risk Management Subcommittees monitor risks from a broader perspective and provide cross-sectional supervision for risks raised by departments, and they also consider and implement countermeasures.

At each meeting, the Risk Management Committee monitors and evaluates risks based on review sheets covering various risks and reports from each risk management division and Risk Management Subcommittee, and deliberates on how to control key risks identified in the process. The results of deliberation by the Risk Management Committee are reported to the Board of Directors, which bears responsibility for ensuring risk governance by verifying the adequacy of the risk management system and the effectiveness of controls over material risks.

Risk Management Committee

- Chairperson: President
- Members:
  Members of the Management Meeting; chairpersons of each risk management subcommittee; general manager of the Internal Audit Office; and full-time auditor (observer)
- Roles:
  1. Monitor important risks and formulate a control plan
  2. Monitor risks reported by subcommittees and divisions
- Convenes:
  Once a quarter in principle and additionally as required

Framework of the Risk Management System (as of June 21, 2024)



Roles of the Internal Audit Office

The status of risk management at each department is ascertained and verified by the Internal Audit Office during regular internal audits. In fiscal 2023, regular internal audits were conducted under the theme of sustainability*.

*Contribution to a carbon-free society, sustainability of suppliers (subcontractors)

Risk Management Activities

Major Issues Discussed by the Risk Management Committee

In fiscal 2023, the Risk Management Committee conducted a thorough review of the comprehensive list of potential risks. During this review, it identified key risks and issues that required attention and discussed various topics, including strengthening risk management related to generative AI services.

FY2023 Operational Policy for Risk Management

Policy	Outline
Coordination with BCMS	Strengthen coordination with the Risk Management Committee to create a more unified operational structure for the BCMS, launched in fiscal 2022.
Expanded Risk Management Committee	Hold an expanded meeting of the Risk Management Committee by effectively utilizing the Executive Officer Committee to establish risk management and BCMS across the Group.

Business Continuity Management System (BCMS)

To prepare against risks that could hinder business continuity, we have formulated a business continuity plan (BCP) to ensure the safety of all related persons, including employees, through the integrated efforts of all executives and employees. In fiscal 2022, we began operating a BCMS as a mechanism for the effective maintenance and management of the BCP.

Under the BCMS, we laid out an annual plan to periodically review the BCP through PDCA activities (business impact analysis, education, training, internal audits, management review, review, and improvement) and by coordinating with risk management undertaken by the Risk Management Committee. During the review process, we conduct a business impact analysis, from the perspectives of risk assessment and impact evaluation, to investigate and analyze the degree to which each target operation will be impacted in the event a risk materializes and to take concrete measures to strengthen corporate resilience.

Furthermore, to realize a system for rapid business recovery and maintenance, we formulated risk-specific response guidelines based on the BCP Common Version, which describes our basic response policy. The guidelines address the seven risks of natural disasters, infectious diseases, industrial accidents, cyberattacks, terrorism, misconduct, and communication failure. Since fiscal 2023, the scope of the BCMS has been expanded to include domestic Group companies. In addition, to prepare for contingencies, we continue to provide BCMS training for directors and employees, conduct periodic drills, and add to our emergency supplies. In fiscal 2023, we conducted new drills for industrial accidents, cyberattacks, and misconduct, in addition to drills for natural disasters, to strengthen our response capabilities.

Major Business Risks

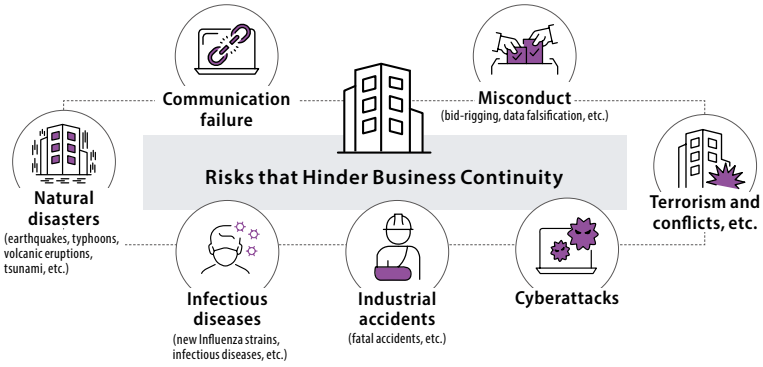
- Business Operation Risks
  - Common to all construction businesses
    - Securing human resources
    - Increase in materials and labor costs and delays in delivery of materials and equipment
    - Overseas business risks
    - Accidents and disasters during construction
    - Unprofitable construction
    - Risks related to litigation, etc.
  - Facilities Construction Business
    - Overabundance of planned projects and increase in property size
    - Response to global challenges
  - Machinery Systems Business
    - Decrease in capital investment
    - Decline in competitiveness
  - Environmental Systems Business
    - Changes in market conditions
    - Long-term business risks
  - Real Estate Business
    - Rent fluctuations
    - Decline in occupancy rate
- Financial and Other Risks
  - Customer credit risk
  - Stock market fluctuations
  - Interest rate fluctuations
  - Seasonal fluctuations in business performance
  - Legal violations
  - Overwork
  - Human rights violations
  - War, terrorism, and natural disasters
  - Climate change
  - Infectious disease epidemic
  - Data security breach
  - System failure
  - Intensifying digital competition

Annual Securities Report for the 100th Business Term (from April 1, 2023 to March 31, 2024) (in Japanese)
https://www.sanki.co.jp/ir/library/doc/securities_R5-4q.pdf

Drills in FY2023

- Industrial accidents
- Cyberattacks
- Natural disasters
- Misconduct

Seven Major Risks that Hinder Business Continuity



Strengthening Risk Management in Overseas Operations

An Overseas Risk Subcommittee was set up within the Risk Management Committee to analyze risks and consider countermeasures. To ensure the safety of employees working outside Japan, we have formulated the Risk Management Manual for Overseas Operations for the head office and overseas bases as well as the Manual to Ensure Safety in Foreign Countries for overseas employees, those traveling overseas on business, and their families. Compliance training sessions for local staff at overseas sites have been conducted since fiscal 2021 to firmly establish governance across the Group. In fiscal 2023, we focused on providing compliance training for managers at our overseas bases in Shanghai and Thailand*.

In addition, our auditors concurrently serve as auditors of Group companies, and we are working to improve our Group management system, including at overseas sites.

Initiatives on Information Security

We have established the Information Security Risk Subcommittee within the Risk Management Committee to control information security measures across the Group and manage risks. We are taking action to respond quickly to cyber attacks by deploying information security software and installing software that constantly monitors the intrusion of malware and other malicious software. We are promoting the use of cloud services to address risks to construction site data storage involving many companies while also providing ongoing training through e-learning on information security for all Company employees and employees of subcontractors.

Risk Management when Using Generative AI Services

Sanki Engineering is promoting the use of generative AI services in its internal operations. We plan to introduce the services in stages and make them available to all Group employees by the end of fiscal 2024.

Since there are potential risks in using generative AI services, such as information leakage and copyright infringement, we are also focusing on countermeasures. In fiscal 2023, we revised our information security measure guidelines regarding precautions for the use of generative AI services. In addition, we are striving to raise awareness of compliance by providing e-learning for all employees to inform them of the inherent dangers and appropriate use of generative AI services.

Drill for walking home in the event of a natural disaster

Risk Management Manual for Overseas Operations

- Response rules and procedures to be followed by the head office and overseas bases in the event of a crisis overseas
- Risks to physical well-being and life, violation of laws and regulations, response to mass media, litigation, etc.

Manual to Ensure Safety in Foreign Countries

- A practical guide on risk avoidance and emergency response for employees working overseas
- Actions required in the event of a terrorist attack or disaster, prevention of damage from crime and other risks, compliance with anti-corruption and other laws, personnel/labor management of locally employed staff, religion, and other related matters

*Sanki Construction Engineering (Shanghai) Co., Ltd., Thai Sanki Engineering & Construction Co., Ltd.

Information Security Rules and Standards

- Information Security Management Rules
- Information System Usage Standards
- Information Security Risk Management Standards
- Information Security Risk Countermeasure Standards