Risk Management

To minimize the various risks surrounding the Yokohama Rubber Group and support our sustainable growth, we manage risks that could have a significant impact on management in a company-wide and cross-functional manner.
We are promoting a management approach that accurately assesses changes in the business environment and takes prompt and appropriate action.

Basic Approach

We are working to strengthen risk management as part of our internal control in order to minimize diversifying risks. We are focusing on identifying events that may have a significant impact on our business, taking preventive measures in advance, and creating a system for prompt and appropriate responses to minimize damage in the event of a serious risk incident.

Currently, there is a need to respond to various changes in the business environment in Japan and overseas, such as growing awareness of human rights and the globalization of business. In addition, the impacts of risks caused by the external environment, such as mounting geopolitical risks, climate change, tight supply of raw materials, and the increasing sophistication of cyberattacks, are also enormous.

In light of these circumstances, we position risk management as one of the most important issues supporting sustainable management, and we are working to maintain and strengthen our company-wide risk management system.

Risk Management System

To strengthen our defense against various risks surrounding our Group, we have established the Risk Management Committee, chaired by the officer in charge of risk management, to manage risks that may have a significant impact on management across our Group and appropriately evaluate and respond to them.

Further, regarding risks with a high degree of importance, including the environment, occupational safety and health, disaster prevention, business continuity plan (BCP), quality management, compliance, information security, and export management, we have put in place a system for the focused management of risks that establishes divisions and meeting bodies specializing in overseeing each risk. This enables us to comprehensively identify risks in our business activities and take appropriate countermeasures.

The activities of the Risk Management, Corporate Compliance, Export Control, Personal Information Protection Management, and Information Security Committees are periodically reported to the Board of Directors. In addition, the activities of other meeting bodies are reported to the Executive Committee as appropriate. Matters that may have a significant impact on management decisions are reported to the Board of Directors.

Fiscal 2025 Results

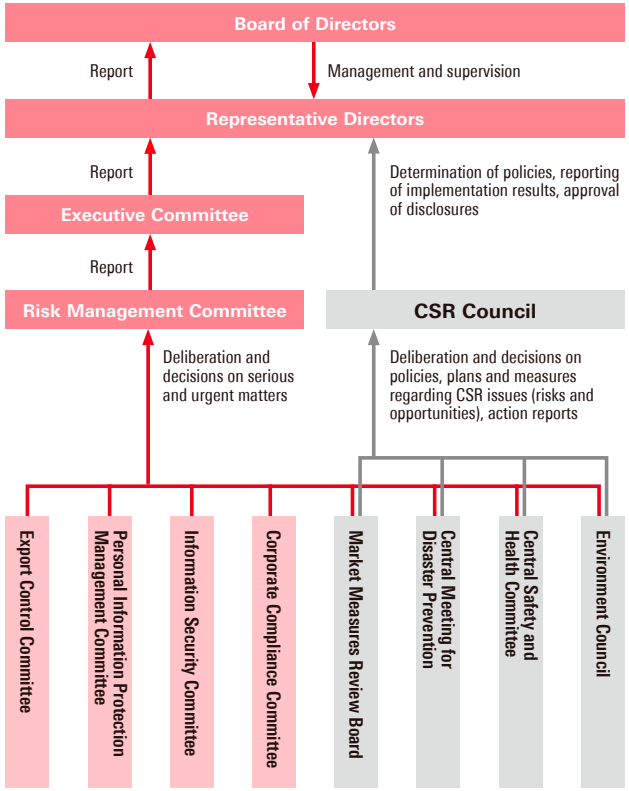
The Risk Management Committee and other committees hold regular meetings twice a year and may hold ad hoc committee meetings based on the standards stipulated in regulations.

Moving forward, we will continue to further promote PDCA activities to identify possible risks, consider countermeasures, inform related parties, and verify them while steadily carrying out our day-to-day initiatives.

Committee Meetings Held in Fiscal 2025 (Including ad hoc committee meetings)

Risk Management Committee	**2 times**
Personal Information Protection Management Committee	**2 times**
Export Control Committee	**2 times**
Information Security Committee	**2 times**

Risk Management System



Risk Management

Information Security Initiatives

We have established the Basic Policy on Information Security, and are implementing a variety of measures to protect customers' personal information and other confidential information from information leaks and cyberattacks, which are becoming more sophisticated and complex every day.

We have also established information security rules, procedures, and global guidelines, and regularly review them in response to changes in the environment surrounding information security.

As the core of the information security system for our entire Group, we have appointed information management officers in each organization, centered on the Information Security Committee, and have built a close communication system.

Furthermore, YRC-CSIRT has been established as an organization under the Information Security Committee. While the Information Security Committee is responsible for formulating and making decisions regarding Group-wide security strategies and policies, YRC-CSIRT carries out front-line operations based on those strategies and policies, including responding promptly to information security incidents, gathering the latest threat intelligence, implementing measures such as information security training, and conducting regular risk assessments. The results of onsite assessments are compiled into reports, and the identified areas for improvement and future action plans are promptly shared with the Information Security Committee. This enables the continuous improvement of highly effective security measures through a unified effort between management and operational teams. In addition, YRC-CSIRT has been a member of the Nippon CSIRT Association (NCA) since 2023, and by deepening information sharing with external specialized organizations and other companies, we are further enhancing our ability to respond to increasingly sophisticated threats.

As a result of these robust systems and ongoing efforts, there were zero major information security incidents in fiscal 2025. Our ongoing initiatives are regularly evaluated through external audits, and we have obtained and maintain TISAX certification, an information security assessment formulated by the German Association of the Automotive Industry. In addition, our information-related subsidiaries have obtained ISO 27001 certification.

Basic Policy on Information Security

1. Protection and appropriate management of information assets
2. Compliance with laws and internal regulations
3. Implementation of ongoing education and training
4. Response to information security incidents and accidents
5. Formulation and continuous improvement of information security management rules

https://www.y-yokohama.com/global/sustainability/governance/risk/

Activities in Fiscal 2025

Fire and Disaster Prevention Initiatives

Learning from the fire that occurred at Yokohama Tire Philippines, Inc. (YTPI)'s production site in the Philippines in 2017, we are working to operate our business with safety as a top priority based on our vow to never cause a fire or accident again. In terms of fire prevention activities, in September 2025, we revised the company-wide Fire Prevention Guidelines, which aim to prevent fires and prevent the spread of fires in the event of an emergency. From fiscal 2026 onward, through the implementation of fire safety inspections, we are continuing to promote preventive management—including measures to prevent recurrence—and making ongoing improvements in management, training, and equipment to ensure that fires do not spread in the event of an emergency. We are also working to strengthen our fire prevention measures to ensure we have a firm grasp of the operations of our newly acquired Group companies, both domestic and overseas. In addition, we conduct fire safety training to ensure that every employee strictly adheres to the rules, and we continuously review standard operating procedures—including those for tasks involving hazardous materials—with a focus on fire hazard prediction through on-the-job observations.

In terms of disaster prevention activities, we revised the Disaster Prevention Guidelines in November 2023 to clarify our preparedness for intensifying natural disasters and infectious diseases occurring over a wide area. Formulated with the aim of maintaining corporate activities based on human life first, these guidelines promote the strengthening of our disaster preparedness capabilities by clarifying the actions that employees should take in the event of a disaster, our disaster prevention system, and the enhancement and management of disaster stockpiles. Disaster prevention drills are also held on a regular basis, and their content, frequency, and the number of participants are confirmed to ensure a quick response to disasters. We also conduct more practical distribution drills, specifically designed for people who may have difficulty returning home.

As a system to establish our central disaster response headquarters of the corporation in the event of a large-scale disaster as well as to collect and share information, we have built a tool that enables multiple means of communication and real-time sharing of information through online meetings, ensuring means of prompt communication that are available even in situations where it is difficult to gather physically.

BCP Initiatives

With regard to the Business Continuity Plan (BCP), we have prepared guidelines including the Basic BCP Guidelines for responding to various destructive and non-destructive disasters, such as infectious diseases. These guidelines are revised as necessary. In fiscal 2025, assuming that our four production sites in Aichi and Mie Prefectures were affected by the Nankai Trough earthquake, we conducted a large-scale BCP drill to verify the procedures for establishing our central disaster response headquarters and ensuring communication using remote tools and emergency communication methods, in accordance with the response manuals for each functional area.

In addition, the IT department is taking the lead in strengthening business continuity planning (BCP) to address cyberattacks, which have become a major social issue.



The large-scale BCP drill

Future Issues and Measures

Since the risks surrounding companies are continuing to increase due to an unstable global situation, the intensification and increasing frequency of natural disasters, and advancement and sophistication of cyberattacks, we recognize that further strengthening of risk management as well as information sharing and communication among departments will continue to be important issues.

Going forward, each department in charge will regularly conduct risk assessments and implement the PDCA cycle to continue improving risk countermeasures, and raise the awareness of each and every employee through BCP drills and information security training and drills.