Risk management

Basic view

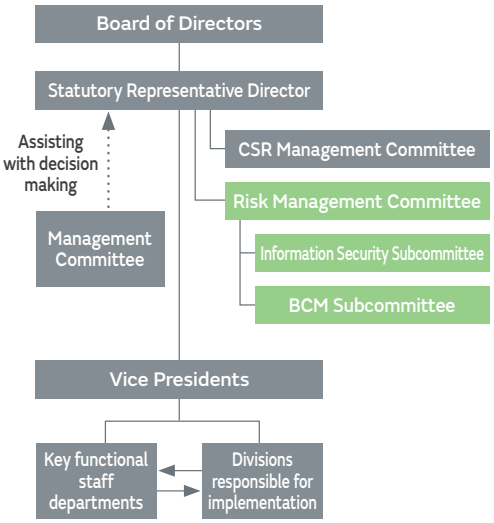
In order to sustainably improve the enterprise value of the entire Group, Murata has built a risk management system to appropriately manage the various internal and external risks related to its business activities. Moreover, we are engaging in activities to reduce loss when risks are discovered that have a significant impact on our business. Examples of these activities include regularly classifying and evaluating each risk concerning our overall business activities and implementing countermeasures in advance according to the priority.

In understanding risks, the key functional staff departments and the business divisions responsible for implementation, which are responsible for each risk, extract the risks that Murata is currently facing or risks that are expected in the near future. The key functional staff departments prevent oversights in risk identification and working to build a system that can appropriately respond to company-wide risks by correctly recognizing: (1) risks which must be identified as company-wide risks from among those extracted by the business divisions responsible for implementation and (2) risks that the key functional staff departments and business divisions responsible for implementation must share and cooperate for. (Refer to the figure Company-wide risk management system below) Moreover, the extracted risks are comprehensively identified and managed by evaluating the importance based on the frequency of occurrence and impact and then displaying those risks on a risk map.

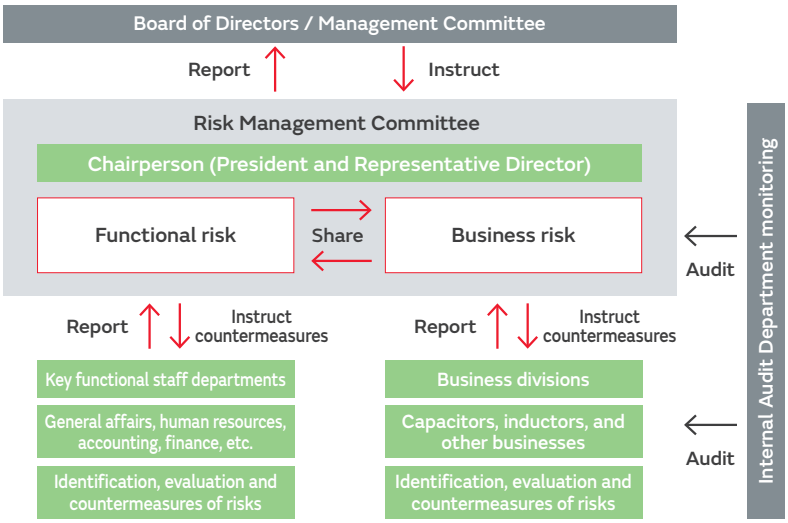
Promotion structure

Murata established the Risk Management Committee to consider measures for countering company-wide risks. The Risk Management Committee became independent from the CSR Management Committee in April 2023 as a committee under the direct control of the Representative Directors. It comprises the President, who serves as the committee's chairperson, and Board Members and Vice Presidents, who are committee members. We have also established the Information Security Subcommittee and Business Continuity Management (BCM) Subcommittee as subordinate organizations to study and take measures to address particular risks.

Internal system diagram



Company-wide risk management system



Business and other risks

Risks that may have a material impact on the company are shown on the following page.

The frequency of occurrence and the degree of impact of residual risk remaining after implementing each risk countermeasure are classified into the three categories: High, Medium, and Low. With regard to the degree of impact, an indicator is selected from the five indicators: "Organizational impact," "Impact on production activities, etc.," "Regulatory/administrative impact," "Impact on business transactions," and "Media/reputational impact." Classification is then made based on the criteria that has been set in advance for each indicator. For more details on each risk and primary response, please refer to the 87th Annual Securities Reports submitted on June 29, 2023.

① External environmental risks		発生頻度	影響度
1	Risks related to global business development	Medium	High
2	Risks related to exchange rate fluctuations	High	High
3	Risks related to financing	Medium	Medium
4	Risks related to fund management	Low	Medium
5	Risks related to environmental regulations	Low	Medium
6	Risks related to climate change	Medium	Medium
7	Risks related to the suspension of business activities due to disasters and infectious diseases, etc.	Low	High

② Strategic risks		発生頻度	影響度
1	Risks related to fluctuations in the demand for our products	Medium	High
2	Risks related to product competitiveness (market share)	Medium	Medium
3	Risks related to dependencies on specific partners and products	Medium	Medium
4	Risks related to M&A, business alliances, and strategic investment	Medium	High

③ Risks related to management foundation		発生頻度	影響度
1	Risks related to information security	High	High
2	Risks related to public regulations and compliance	Low	High
3	Risks related to intellectual property	High大	Medium
4	Risks related to taxation	Medium	Medium
5	Risks related to the hiring and securing of human resources	Medium	Medium

④ Business execution risks		発生頻度	影響度
1	Risks related to the development of new technologies and products	Low	High
2	Risks related to procurement	Medium	Medium
3	Risks related to customer trust	High	Low
4	Risks related to quality	Medium	High

Business Continuity Management (BCM)

Consequently, Murata has devised a Business Continuity Plan (BCP) to ensure that we can fulfill our duty to provide customers with a stable supply of products. We are conducting initiatives to minimize damage and continue business, such as ensuring earthquake resistance and safety for buildings and production facilities, constructing backup frameworks for our communications and information systems, and maintaining supply from product inventory.

Within material procurement, the production locations of material suppliers are stored in a database so that procurement activities are not delayed when a disaster or other risk occurs. We have also formulated an initial response system and a response flow for expected risks to implement a rapid initial response. Furthermore, in order to ensure stable procurement of important materials, we are promoting measures such as implementing a multi-vendor system, confirming the BCP implementation status of our vendors, and ensuring sufficient materials inventory to cover the expected recovery period, if risks materialize.

Additionally, we must promote the establishment of BCM organizations to handle risks that could occur at the global level, prevent risks that could impair Murata's business continuity, and minimize loss if risks should materialize. To this end, Murata is taking measures such as verifying the effectiveness of its BCP through periodic drills at its domestic and overseas offices and plants. We recognize that preparing for the Nankai Trough Earthquake, which would be especially massive and damaging, and geopolitical risks is of utmost importance. We continue to promote measures in order to fulfill our obligations as a components manufacturer to continue supplying products.

Topics Establishment of the Tokyo Logistics Center

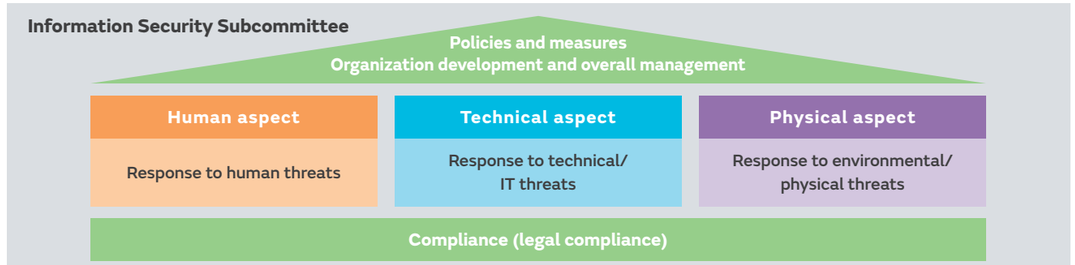
In order to prevent shipping operations from being suspended due to events such as recent natural disasters and pandemics caused by infectious disease like COVID-19, Murata established its second logistics center, Tokyo Logistics Center, in Nagareyama City, Chiba Prefecture, in December 2022. Together with the existing Osaka Logistics Center in the Kansai region, the establishment of this new logistics center in the Kanto region means that Murata now has two logistics centers in Japan, which will enable us to ensure the smooth supply of products to customers and stable distribution in the event of a natural disaster or other misfortune.

Information security management

Murata recognizes that risks related to information security are matters that may significantly impact its operations, and that it is crucial to protect the company's trade secrets and information provided by its business partners and customers. Risks related to information security, such as information leaks caused by internal fraud targeting information retained by companies and disruptions to business activities caused by cyber attacks, have been increasing in recent years. Hence, Murata incorporates recent risk trends and related guidelines from Japan and overseas based on international standards (ISO 27001) to implement information security management.

Information security system

Murata established the Information Security Subcommittee as a lower branch of the Risk Management Committee. We aim to minimize risks by running through the information security risk management PDCA cycle every day, addressing human, technical, and physical aspects, in order to prevent potentially serious incidents from happening, under the management of officers responsible for information security (executive officers and the Corporate Division ESG/HR Management Department Manager).



Human aspect

Information security related rules are described in employee handbook and the pledge with employees. In addition, the Information Security Guidebook, which explains the rules in an easy-to-understand manner, is written and distributed in Japanese, English, and Chinese so that all officers and employees in Japan and overseas can understand information security and handle information in the proper way. The company also implements annual training for all employees to increase their awareness of information security, phishing email drills, in-house training by employee level (new employees, etc.), and information security training for telecommuting employees.

Global training ratio* for fiscal 2022 = 96%

*Training ratio = (Number of sites that have conducted training) / (Total number of sites)

Technical aspect

In order to deter leaks of Murata's confidential information and personal information as well as interruptions of business activities due to cyber attacks, we continue to strengthen anti-malware measures, hardware asset management, firewall construction, Internet communication checks, ID management, system access controls, and diagnosis and countermeasures for vulnerabilities in current information systems. Moreover, we are globally collecting and monitoring various logs to construct a system for responding to incidents which may become a security accident. In particular, we continue to strengthen security at the production sites that form the basis of our business activities, and promote responses and countermeasures to constantly changing cyber attacks and risks to maintain a stable and safe production system.

Physical aspect

To prevent unauthorized intrusions into premises at offices, sites and affiliated companies in Japan and overseas, access control of people and vehicles is carried out at all times. Security zones are established within business sites according to the level of security control, and various measures including access controls using ID cards, etc. are implemented in highly secure zones to prevent unauthorized internal and external intrusions.

Moreover, in order to continuously improve the physical security level, we periodically diagnose and audit the operating conditions from the perspectives of early detection and evidence accumulation measures in addition to restricting people's movements and implementing preventive measures, and we are promoting the construction of a system to horizontally deploy responses to accidents and incidents, which may escalate into accidents, to other offices, sites and affiliated companies.

Topics Achieving TISAX label

In response to the growing importance of information security in the automotive industry, our major domestic and overseas sites (including our headquarters) have achieved Trusted Information Security Assessment Exchange (TISAX) label, an information security evaluation conducted by the German Association of the Automotive Industry. Going forward, we will continue to get more of our sites certified in addition to conducting our usual internal and external audits and examinations, in order to spread awareness and enhance information security management.

For details regarding the status of TISAX label achievement, please see here. ▶