Risk Management

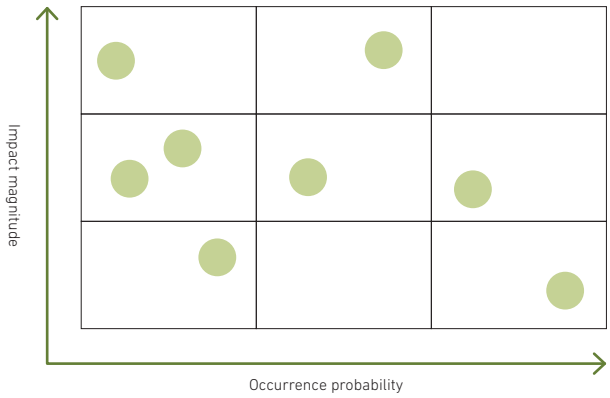
MHI Group: Risks and Responses

Key risks that could, in the assessment of MHI Group's management, materially affect the Group's financial condition and/or operating performance, including cash flows, are tabulated below (forward-looking statements are based on judgments as of March 31, 2024).

We have established management processes for identifying, assessing, and cataloging operational risks on an annual basis. To identify relevant risks, we prepare a comprehensive list of risks with input from external experts that covers the risks generally relevant for companies, including changes in the external environment. Based on this list, we identify specific risks that have the potential to occur within the next 10 years. We then assess the probability of such risks occurring and the magnitude of impact when they materialize, taking into account the effectiveness of countermeasures, and organize them into a risk map showing quantitative risks and qualitative risks. The identified and visualized risks are reported to the Board of Directors and incorporated into the business planning process and its follow-up cycle.

The countermeasures in the table below are examples of specific measures we have already implemented in response to key risks. They are factored into the key risks' potential impacts on our financial condition and/or operating performance. In addition to the countermeasures mentioned below, we engage in risk management, including risk avoidance and reduction, according to the type and nature of various risks, including those specific to individual business units that require attention.

Risk Map (image)



Key risks	Potential impacts on financial condition and/or operating performance	Countermeasures
Changes in the business environment	• Constraints on negotiations and supplier selection, etc. due to progress of economic decoupling caused by the U.S.–China conflict, the introduction of new foreign and security policies, or changes in existing policies, etc. • Rapid fluctuation of exchange rates, rising raw material prices, and logistical stagnation and disruption • Growing labor shortages, intensifying competition to attract human resources, and increasing labor mobility in Japan • Contraction in businesses' scale and/or inability to recoup invested capital due to a reduction in demand for products or services caused by growing environmental consciousness • Reduction in order bookings or a slowdown in service businesses in response to, e.g., intensification of competition or a sharp drop in demand for electric power derived from fossil fuels • Energy transition may evolve more slowly than assumed when we developed the business plan • Recognition of impairment losses due to mergers, acquisitions, and/or alliances' underperformance of expectations	• Collection of information on global conditions and laws and regulations of each country, and implementation of action based on this • Placed priority on new functions/solutions that incorporate external expertise and are predicated on maintaining or strengthening product competitiveness in terms of, e.g., performance, reliability, price, and/or eco-friendliness through R&D or capex • In April 2024, we established the GX (Green Transformation) Solutions segment to strengthen our project management and engineering functions related to energy transition initiatives. • Facilitated PMI* through, e. g., better up-front screening and monitoring of M&A deals/alliances *PMI: Post Merger Integration

Key risks	Potential impacts on financial condition and/or operating performance	Countermeasures
Disasters	• Destruction of or damage to production facilities, supply chain backups or disruptions, shortages of, e.g., parts or materials required for production, interruption of services, reduction in production capacity utilization, plant shutdowns, loss of backup production capacity or suppliers, and/or losses in excess of insurance coverage due to a disaster in Japan or Thailand, where production capacity is concentrated, or anywhere else operations are located globally	• Maintained adequate insurance coverage, collected information on conditions and safety in every country in which we operate, took precautions based on that information and communicated with relevant government authorities • Utilized disaster preparedness/response tools, established/maintained lines of communication, formulated/updated business continuity plans, formulated/updated working environments and systems, inspected plants, upgraded facilities' earthquake-resistance, periodically conducted emergency drills
Product/service-related problems	• Cost overruns, payment of damages to customers, impairment of public reputation and/or loss of societal trust due to, e.g., the occurrence of various problems with or arising from products, cost increases attributable to, e.g., changes in specifications or process delays, unforeseen problems related to construction or sourcing of, e.g., parts and materials, and/or impacts on MHI's production activities or products/services' availability to customers resulting from a supplier's inability to supply specific parts/materials or the occurrence of labor shortages among partners due to stricter labor-related laws and regulations • Deterioration of business conditions or changes in business policies among important and difficult-to-replace customers, suppliers, and business partners	• Instituted and enforced various regulations, built and strengthened the operational risk management regime • Individually screening incoming orders before acceptance, monitoring fulfillment process after acceptance • Conducting training for project/department managers, holding product safety seminars on ongoing basis • Implemented recurrence prevention measures, including by recapping causes of, and corrective action in response to, major losses incurred on previous projects and incorporating the information into internal training programs ▶ For details, please refer to "Business Risk Management" (P75).
Intellectual property disputes	• Liability for damages and/or loss of right to use certain technology due to adverse outcome of, e.g., litigation related to intellectual property (IP) infringement • Obstruction of business operations due to inability to in-license technology from third party	• Avoiding IP disputes by thoroughly researching IP owned by others at the product planning, design, and production stages • Upgraded IP staff's expertise through education and HR development
Cybersecurity problems	• Major loss of competitiveness, impairment of public reputation and/or loss of societal trust in connection with information leak due to, e.g., increasingly sophisticated/malicious cyberattacks • Disruption of operations due to, e.g., disablement of computers or servers • Investigations by authorities, claims for damages by, e.g., customers	• Implemented cybersecurity controls (standards, safeguards, self-assessments, internal audits), incident response measures, etc. by building a cybersecurity regime under direct supervision of the CTO ▶ For details, please refer to "Cybersecurity" (P76).
Legal/regulatory violations	• Administrative sanctions imposed by government authorities, including correction orders, penal fines, non-penal fines, suspension of operations, and/or export bans in the event of legal/regulatory violations; claims for damages from authorities or interested parties • Disruption of operations, impairment of public reputation, and/or loss of societal trust	• Instituted and enforced the MHI Group Global Code of Conduct and various regulations applicable to all Group personnel • Regularly holding Compliance Committee meetings, established internal compliance reporting program • Disseminating messages from management officers on strict legal/regulatory compliance, conducting various internal trainings on an ongoing basis, augmenting training curricula, conducting internal audits ▶ For details on strengthening compliance, please refer to "Compliance" (P77).

Basic Approach to Business Risk Management

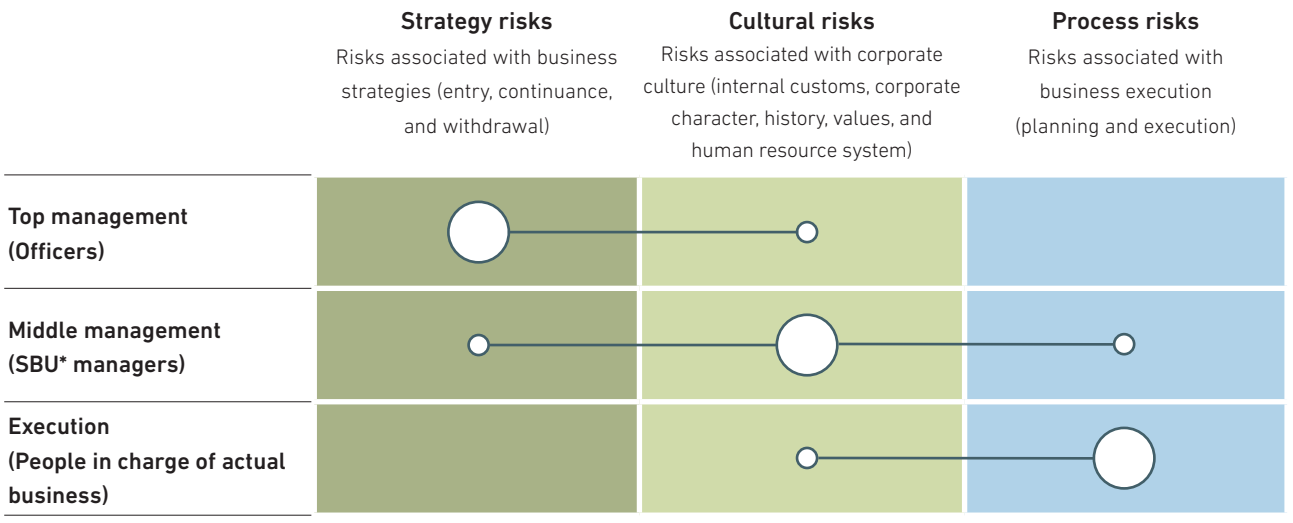
Throughout its history, MHI Group has achieved sustained growth by taking up diverse new challenges and initiatives in numerous business areas. At the same time, on occasion we have experienced losses on a large scale.

For MHI Group to mark sustained growth amid an ever-changing business environment, it is necessary to continue to take up challenges in new fields, new technologies, new regions, and new customers as well as to improve and strengthen operations in its existing business markets. Such challenges will entail business risks, and a company's ability to curb risks wields significant influence on its business results and growth potential.

To link challenges of this kind to the next leap into the future, MHI Group, applying its past experience and lessons learned, has established the "Business Risk Management Charter" and will promote the creation of mechanisms that will ensure the effective execution of business risk management and the cultivation of a culture responsive to risks. MHI Group will also reinforce advanced, intelligent systems and process monitoring, both of which support top management's strategy decisions. Through these approaches, we will pursue "controlled risk-taking" that will enable us to carry out carefully planned challenges toward expanding our business.

We believe that risk management is a part of governance and functions only when the elements of systems and processes, corporate culture, and human resources are in place. For our Group to succeed in the global market, we need to take bold and daring risks, but we also need to manage those risks. That is the perfect combination for continually increasing our corporate value. In this sense, it is important that all business participants, from people engaged in the actual business to management, comprehend and control risks in business, from processes to strategies. For details, please see the chart below (Matrix of Business Risk Management).

Matrix of Business Risk Management



*SBU: Strategic Business Unit (business unit in the Strategic Business Assessment System)

Business Risk Management Structure

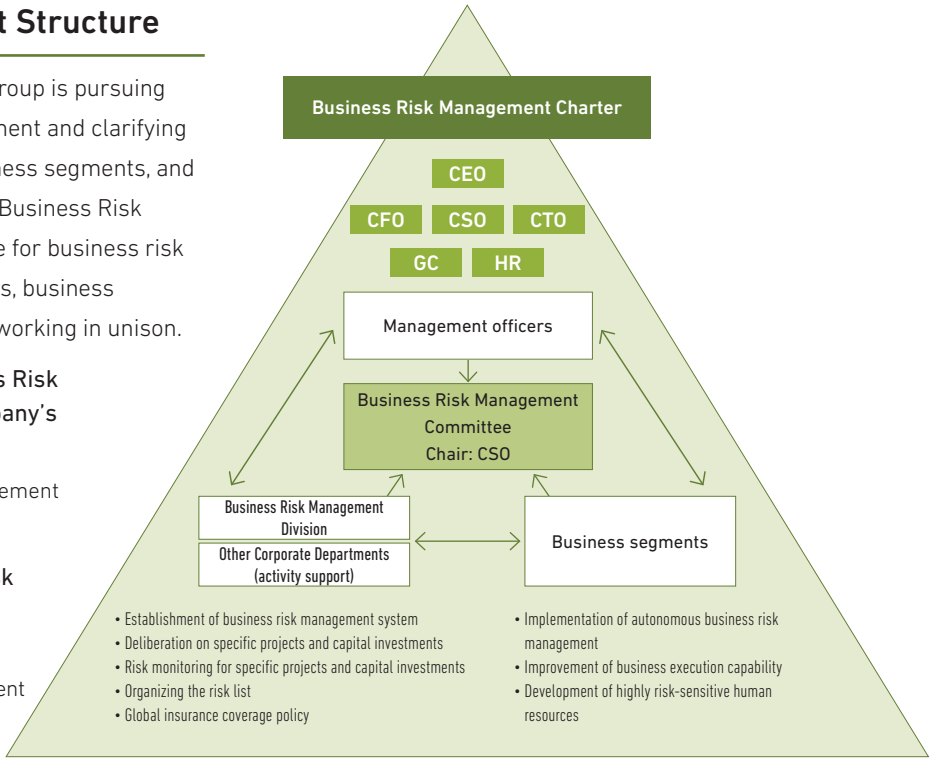
Through the following measures, MHI Group is pursuing more organized business risk management and clarifying the roles of management officers, business segments, and corporate departments. In addition, the Business Risk Management Department is responsible for business risk management, with management officers, business segments, and corporate departments working in unison.

1 Observe and practice the Business Risk Management Charter as the Company's foremost set of rules

- Clarify, observe, and practice risk management targets, etc.

2 Hold meetings of the Business Risk Management Committee

- Share information on important risks and discuss response policy by top management
- Report particularly important matters to the Board of Directors
- Held four meetings in FY2023

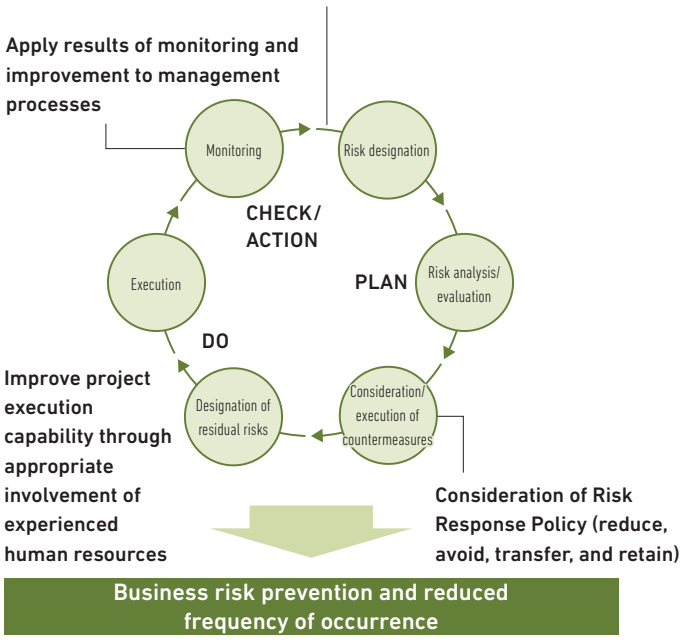


Business Risk Management Process

With the Business Risk Management Division acting as the responsible department, MHI Group engages in business risk management activities bringing together management, business segments, and corporate departments.

The chart on the right (Business Risk Management Process) outlines specific activities. In addition to improving systems and processes to prevent business risks, reduce the frequency with which such risks manifest themselves, and consider and implement measures, we develop human resources in charge of business risk management and cultivate a culture of responding to risks through such efforts as providing training for SBU manager candidates.

Business Risk Management Process



Cybersecurity

MHI Group, which provides critical infrastructure to society, recognizes cybersecurity risk as one of its most important risks. With this in mind, we established a cybersecurity basic policy and a cybersecurity strategy.

The Group regularly monitors this risk. The President and CEO supervises the cybersecurity strategy, and the CTO reports the results of discussion in the Cybersecurity Committee in a timely manner to the Executive Committee and Board of Directors. Based on the policy and strategy, a cybersecurity program has been implemented under the control of the CTO to minimize the risk of cyber incidents. Cybersecurity governance, incident response, and education and training are maintained and performed under this program. At the same time, MHI Group is contributing to the establishment of a global cybersecurity framework.

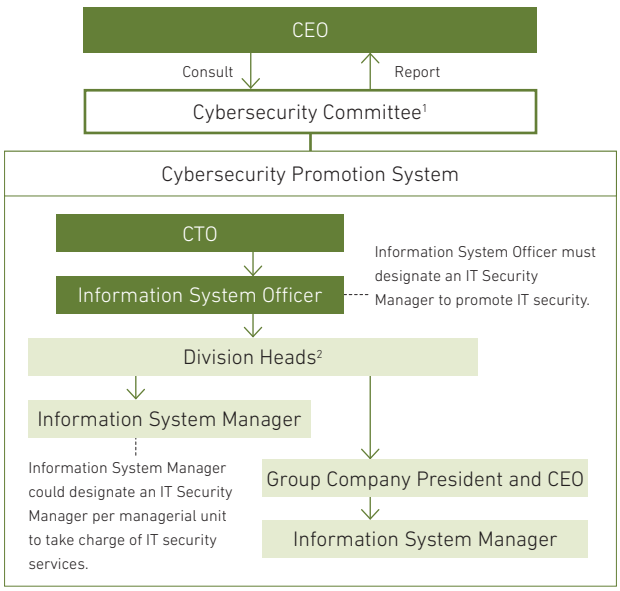
Cybersecurity Governance

Based on the NIST CSF[1], MHI Group has established cybersecurity standards and implemented multi-layered defense measures against cyberattacks. We also perform periodic self-assessments and internal audits.

Emergency responses are taken without hesitation when signs of a security risk are found. Furthermore, we are revising standards based on MHI Group's issues by referring to the state of formulation and revision of guidelines by governments and organizations, such as the Cybersecurity Management Guidelines announced by the Ministry of Economy, Trade and Industry. With respect to control systems for our products and services, we have built a framework that controls cybersecurity risk and will work with business partners to upgrade the cybersecurity capabilities and capacity of our products and services on a regular basis. By driving the development of next-generation cybersecurity solutions, MHI will help build a safe, secure society.

1 NIST CSF: National Institute of Standards and Technology Cyber Security Framework

IT Security Management System



1 Established August 8, 2023

2 Division Head: The Head of domain, and the Head of segment. The Head of Digital Innovation HQ for the corporate division.

Response to Cybersecurity-Related Incidents

In the event of a cybersecurity incident, a CSIRT (Computer Security Incident Response Team) immediately reacts to the incident, handles analysis and examination of the incident, recovers systems, and carries out further preventive measures. Incidents are reported to stakeholders as needed, including concerned government agencies. Serious incidents are internally reported to directors, and measures are taken in accordance with our crisis management system to swiftly recover operations according to our business continuity plan.

Due to the increased frequency of ransomware attacks requiring swifter management decisions and communication, we confirm and revise the response capabilities and issues of organizations in an emergency through incident response drills that include management.

Cybersecurity Education and Training

MHI Group regularly provides cybersecurity education and training to all employees as warranted by their respective roles with the aim of maintaining and improving their cybersecurity literacy. We also aim to cultivate engineers capable of both safety- and security-minded product and service development.

Contributing to the Establishment of a Global Cybersecurity Framework

Through participation in the Study Group for Industrial Cybersecurity[2], the Charter of Trust[3], promotion of the Declaration of Cyber Security Management 2.0, and other cybersecurity initiatives, MHI Group is contributing to the establishment of a global cybersecurity framework.

2 An initiative by the Ministry of Economy, Trade and Industry to examine industrial cybersecurity measures.

3 An initiative by private corporations to build trust in cybersecurity.