Risk Management

Basic Stance

To minimize the impact of constantly diversifying risks, DENSO is working to strengthen its risk management structure as a part of internal controls. Specifically, we have divided matters that have the potential to damage our businesses into "risks," which refer to circumstances where such matters have yet to manifest, and "crises," which refer to states of emergency where such matters have manifested. Based on these classifications, we are focusing our efforts on implementing preventive measures, which stop risks before they occur, and swift and accurate initial-response and recovery measures, which are deployed in the event a crisis occurs, while taking steps to minimize and mitigate crises when they emerge.

Promotion Framework

DENSO has established the Risk Management Meeting, chaired by the chief risk officer (CRO) responsible for overseeing risk management across the Group, to promote initiatives that include reviewing progress in improving the Group's risk management systems and frameworks, and deliberating and providing direction on priority activities in light of internal and external environments and trends.

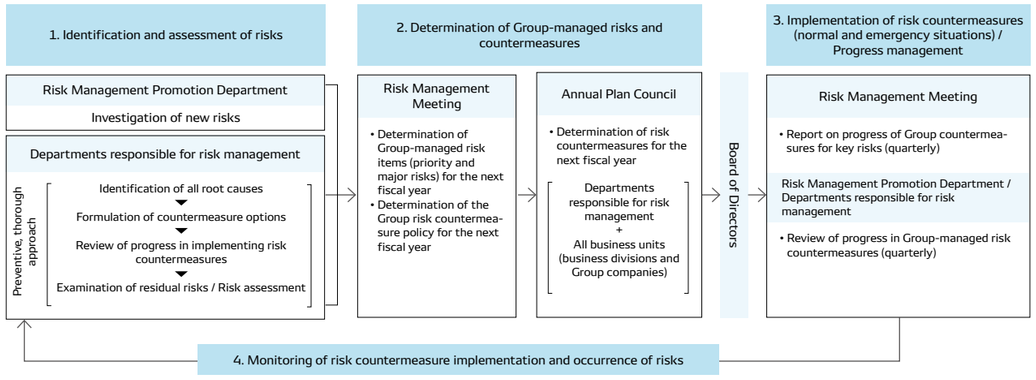
Ascertaining Risks and Clarifying Response

DENSO makes efforts to actively ascertain the risks it faces and manage these risks from the perspectives of prevention and damage mitigation. Every year, risk assessments are carried out by each functional division, business unit, overseas regional headquarters, and Group company.

The Company has identified risks that could potentially damage its operating capabilities, credibility, assets, and production activities, as well as the environment, based on the surrounding business environment. The Company designates responsible departments to examine the reasons for the occurrence of such risks and for the expansion of damages after occurrence, thereby clarifying preventive measures, initial response, and recovery efforts for these risks. Based on the implementation status of response and other measures, the Company has also assessed the scale of remaining risk factors for each risk based on the perspectives of level of impact and frequency of occurrence. In particular, DENSO is identifying risks for which remaining risk factors are significant and toward which it invests resources to promote countermeasures as "key risk items." Also, with regard to its response measures for key risk items, DENSO has established quantitative KPIs for Companywide targets, and the status of initiatives based on these KPIs is also confirmed by the Board of Directors.

For fiscal 2026, the Company has determined 37 major risk items and, among these, six key risk items. DENSO will continue to revise these major risk and key risk items appropriately based on the results of risk assessments.

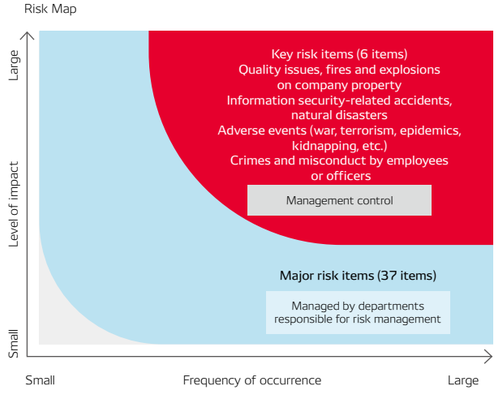
Risk Management Process



Major Risk Items and Key Risk Items

Factors	Risk Items
Internal factors (accidents and mistakes)	Environmental pollution, work-related accidents, fires and explosions, quality-related issues, information security-related accidents, personnel- and work-related incidents, traffic accidents, etc.
Internal factors (legal violations)	Violation of the Antimonopoly Act, inappropriate employee dispatch or use of contract work, violation of product laws and regulations, violation of anti-bribery laws, etc.
External factors (natural disasters)	Earthquakes, typhoons, concentrated heavy rains, lightning strikes, etc.
External factors (political and social)	Product liability litigation, supplier-related issues, incidents or other emergencies (infectious diseases, wars, terrorist attacks, etc.)

Risk Map



DENSO Integrated Report 2025
Corporate Governance

Status of Responses to Key Risks

Major Risk Items	Risk Details	Responses
Quality issues	Quality issues that could lead to large-scale recalls may result in loss of trust from end-users and customers, potentially causing significant costs and a decline in sales.	We incorporate safety designs, such as fail-safe mechanisms to prevent serious failures, design products with repairability in mind to minimize damage in the event of a defect, utilize big data, such as vehicle operating conditions at the time of failure, for early resolution, and promote efficiency in data analysis through AI technology.
Information security-related accidents	Advancements in autonomous driving and IoT have increased the threat of cyberattacks on vehicles, production facilities, and other systems. In the event of a cyberattack far exceeding expectations, there is a risk of adverse impacts on the functions of automotive products, production stoppages, and leaks of confidential information, potentially resulting in loss of competitiveness and damage to reputation. Furthermore, the proliferation of AI is increasing risks, such as confusion caused by false or misleading information, legal violations, infringement of rights, and information leaks.	Please refer to "Strengthening Our Information Security Framework" below.
Natural disasters	Global warming is raising concerns over the increased frequency and severity of natural disasters, such as floods and heavy rain. In Japan in particular, many business sites are located in areas designated for promoting countermeasures against a potential Nankai Trough earthquake. In the event of a natural disaster, delays or errors in the initial response could endanger employees' lives and halt production and delivery activities.	We are engaged in disaster mitigation measures, such as formulating business continuity plans (BCPs) and emergency action manuals. We also aim to strengthen our response capabilities by repeatedly conducting various training and awareness activities to further enhance each employee's awareness of disaster preparedness.
Fires and explosions on company property	In the event of a fire or explosion at a plant, delays or errors in the initial response could endanger employees' lives and halt production and delivery activities. Such incidents could also cause damage to the local communities near the plant.	We conduct regular inspections and maintenance of equipment to minimize negative impacts on business operations. We also aim to strengthen response capabilities by improving disaster awareness among employees through repeated training and awareness activities so that all employees can take appropriate initial action in the event of an emergency.
Adverse events (war, terrorism, epidemics, kidnapping, etc.)	The weighting of overseas markets in DENSO's production and sales activities has been increasing year by year. Overseas business operations inherently involve risks, such as war, terrorism, epidemics, and kidnapping, and if any such incident occurs, the lives of employees and their families could be endangered. Such incidents are also likely to hinder the normal conduct of business activities.	We strive to gather timely information from internal and external sources, quickly share risk information with relevant parties, enhance alerts for employees on overseas business trips, and strengthen pre-departure training for overseas assignments to raise employees' risk awareness. We have introduced a common self-assessment protocol to confirm preparedness during normal times at all Group companies, aiming to enhance the Group's overall crisis management framework.
Crimes and misconduct by employees or officers	If an employee or officer commits a crime or an act of misconduct, it may be reported by the media or disseminated through social media and other channels, potentially causing the Company to lose credibility. In some cases, the Company may also become a party to lawsuits and other legal proceedings.	We have formulated and shared a Code of Conduct for employees, and continuously deliver messages from the CRO and CCO, as well as provide various training and awareness activities for officers and employees. We also undertake monitoring efforts to detect early signs of issues. At the same time, we have established an internal reporting system to capture problematic behavior and other concerns.

Strengthening Our Information Security Framework

With the advancement of autonomous driving and IoT, addressing cyber risks involving vehicles, production facilities, and other assets has become a major challenge. To ensure vehicles can be used safely and securely, we are developing and reliably integrating technologies to protect in-vehicle products, such as advanced driver assistance systems and autonomous driving systems, from cyberattacks, while establishing internal rules and processes in compliance with laws and regulations in each country, and training core personnel responsible for product security. For plant and supply chain security, we are implementing multi-layered defenses using the latest IT technologies, helping suppliers improve their security standards, and building a framework to ensure uninterrupted production and supply. In addition, to objectively evaluate and validate these activities, we are working to obtain international security certifications, such as Trusted Information Security Assessment Exchange (TISAX), which is administered by the German Association of the Automotive Industry (VDA), and the automotive cybersecurity standard ISO/SAE 21434.

Furthermore, the proliferation of generative AI is increasing the scope of risks, such as confusion caused by false or misleading information, legal violations, infringement of rights, and information leaks. While leveraging AI to improve operational efficiency, DENSO is also working to reduce risks by building frameworks for security reviews and monitoring when using cloud services or AI. We have also formulated guidelines for the use of generative AI and are providing training to employees to improve their literacy in information security, including AI-related risks.

For more information on Risk Management, please see the following website.
https://www.denso.com/global/en/about-us/sustainability/governance/risk/