

Risk Management

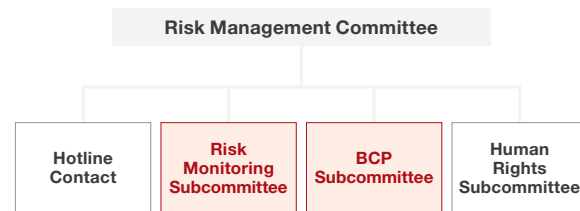
Risk management system and operation

We have established Crisis Management Regulations with the aim of avoiding the occurrence of risks in the IDEC Group and minimizing damage in the event of actual occurrences.

We established the Risk Management Committee as a specialized committee under the Sustainability Committee, chaired by the CEO, to continuously oversee the Group's risk management during normal times and respond to risks that occur. We have also established the Risk Monitoring Subcommittee, BCP Subcommittee, and Human Rights Subcommittee (all subcommittees under the Risk Management Committee) to identify and assess risks throughout the IDEC Group, monitor efforts to reduce risks, formulate business continuity plans, and work to address human rights issues.

A Hotline Contact has also been established within the Committee to develop whistleblowing channels and respond to whistleblower reports.

Risk Management System



Details of these initiatives are reported to the Sustainability Committee, which meets twice a year, and the committee then reports to the Board of Directors. The Risk Management Committee reports directly to the Board of Directors on important events such as whistleblowing reports, ensuring that risk information is reported appropriately to management.

Business continuity planning

To prepare for natural disasters such as earthquakes, which are one of the IDEC Group's high risk events, we have established a subcommittee within the Risk Management Committee to formulate business continuity plans (BCP). The subcommittee works in cooperation with relevant parties in the manufacturing division and target sites to formulate basic policies, initial response flowcharts, and business continuity plans for in the event of a disaster.

In addition, we map out the initial actions to be taken by each emergency task force member in a disaster, and create manuals and checklists for guiding those actions. We also routinely review our disaster countermeasures, and use the intranet to communicate information for raising the disaster prevention awareness of all employees.

Our basic policy on crisis response

- Place top priority on the safety of employees and their families
- Establish mechanisms and organizational structure that will enable us to maintain quality to meet customer needs with safe and ANSHIN products and services, and avoid delaying the supply of products, even in the event of an emergency
- Recognize the importance of daily readiness and training, and establish a strategy and organizational structure that takes crisis response into account

Information security initiatives

We recognize the important information assets handled in the course of our business activities, and strengthen the IDEC Group's management system for information security by systematizing basic policies, management regulations, and procedures for the appropriate handling of information assets.

We regard risks to information security as one of the most important types of risks, and are working on measures to reduce them. In addition to technical measures, we are also implementing management measures such as employee education, and promoting employee awareness through e-Learning courses for all employees and information disclosure on the intranet.

We are working to build an organizational structure in which, in the event of an incident, employees promptly report the incident, take appropriate initial measures to minimize the spread of damage, and report to management and the Risk Management Committee. Going forward, we will continue to organize a system of relevant departments throughout the Group, in addition to the IT department, to take appropriate measures that take into account the impact on stakeholders, including customers and suppliers, as well as those within the Group.

Information security e-Learning attendance in FY2024 (Japan)

	Number of trainees (%)
First session	1,259 (94.0%)
Second session	1,286 (93.8%)
Third session	1,238 (91.2%)
Fourth session	1,155 (85.4%)

Risk map and identification of high-risk events

The Risk Monitoring Committee regularly identifies and evaluates risks based on the assumed risk events that may negatively impact the IDEC Group's continued business expansion and corporate value enhancement. Concerning each risk event, an evaluation questionnaire is conducted using the "probability of occurrence," "magnitude of damage" and "impact" as measures, and the results are plotted on the risk map relative to the assessment.

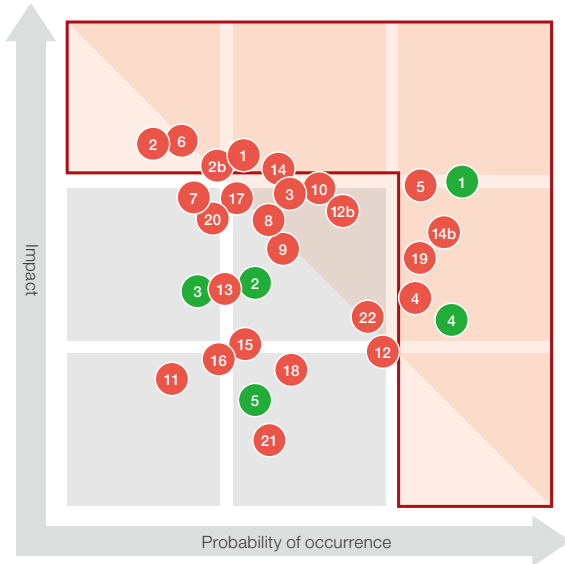
The risk events evaluated include climate change risks that the Environmental Strategy Committee has judged to be significant issues. Also, risk events that have a high probability of occurrence are considered high-risk events. Each department responsible for a particular high-risk event is assigned a risk reduction target, and gauges its progress toward the target on a semiannual basis.

Major responses to high-risk events in FY2024

No	Risk event	Actions
1	Damage to IDEC's sites in Kansai region in Japan by an earthquake with a seismic intensity of lower 6 or higher	<ul style="list-style-type: none"> ■ Formulated business continuity plan and improved manufacturing site's emergency response capabilities ■ Reduced risk by taking out an appropriate insurance policy ■ Developed an emergency contact network and a means of checking employee safety
6	Occurrence of a serious product accident that could affect the human body	<ul style="list-style-type: none"> ■ Instituted system for monitoring complaints/failure reports from the market to enable early detection of and response to major complaint-generating issues ■ Evaluated risks in new product development and implemented measures to prevent issues during production
19	Leakage of critical corporate information, third-party confidential information, and personal information	<ul style="list-style-type: none"> ■ Technical measures for information security ■ Increased our knowledge of how to prevent information leaks

* Item numbers correspond to risk event numbers on the following page.
* See the following page for explanations of the risk map and high-risk events.

Risk Map in FY2024



* Climate change risks reflect events that the Environmental Strategy Committee assessed as high-risk. 25B
 * Risks are evaluated on a short to medium-term basis. Long-term climate risks have been re-evaluated on a short to medium-term basis.
 * Risks inside the red box are judged to be high-risk events.

Risk category	No	Risk event	FY2024 risk assessments	Year on year comparison
External factor risks	1	Damage to our Kansai region sites in Japan by an earthquake with a seismic intensity of lower 6 or higher.	Given the risk of a Nankai Trough earthquake, the probability of occurrence has increased since FY2023, and continues to be assessed as a high-risk event.	↑
	2	Conflict or terrorist attack in the local area of IDEC sites.	Assessed as a high-risk event, as in FY2023.	—
	2b	Impact on our overseas staff and site operations due to interstate affairs or public disorder.	The probability of occurrence has increased slightly, and is assessed as a high-risk event, as FY2023.	—
	3	Occurrence of cluster infections at our sites.	Impact was assessed as lower due to changes such as implementation of infection prevention measures and change of awareness on viral infection.	—
Internal factor risks	4	Product specification change caused by external factors. (part obsolescence, procurement difficulty)	Both degree of impact and probability of occurrence remain high as a result of specification changes, due to difficulties in procuring electronic components. The risk level is assessed as high.	↑
	5	Difficulties in procuring parts that could lead to long delivery delays.	Both degree of impact and probability of occurrence remain high as a result of specification changes, due to difficulties in procuring electronic components. The risk level is assessed as high.	—
	6	Occurrence of a serious product accident that could affect the human body.	Assessed as a high-risk event with considerable impact, as in FY2023.	—
	7	Fraudulent representation of quality through falsification of product performances and data.	It is assessed that the degree of impact will increase in global business.	↑
	8	Distribution of products containing prohibited substances.	Assessed as being at a level similar to FY2023.	—
	9	Strategic investment risk. (financial impact of M&A, corporate alliances, and other strategic investments)	Assessed as being at a level similar to FY2023.	—
	10	Occurrence of a severe or more industrial accident.	The probability of occurrence has increased in comparison with FY2023 due to the impact of the workplace environment.	↑
	11	Sabotage, strike-related business outage.	The probability of occurrence is assessed as being lower than FY2023.	↓
	12	More than half a day of infrastructure outages caused by system and network failure, etc.	We reaffirmed the impact of network downtime, and evaluated the degree of impact as being higher than FY2023.	↑
	12b	Long-term network outage due to cyberattack.	The impact of long-term network outages is assessed as significant.	—
	13	Suspension of sales and claims for damages due to infringement of other companies' intellectual property rights.	Assessed as being at a level similar to FY2023.	—
	14	Inaction on human rights issues. (child/forced labor, etc.)	Assessed as having a significant impact due to growing awareness of human rights issues in global business.	—
	14b	Decline in employee morale due to harassment.	The frequency of occurrence is assessed as going to increase from FY2023 due to the impact of the workplace environment.	↑
	15	Tax penalty due to improper handling of accounting and tax affairs.	Assessed as being at a level similar to FY2023.	—
	16	Large-amount embezzlement, malpractice, and bribery by employees.	Assessed as being at a level similar to FY2023.	—
	17	Insider trading by senior executives.	The probability of occurrence is assessed to increase slightly due to the business performance.	↑
	18	Occurrence of events in breach of antitrust and subcontracting act.	The frequency of occurrence is assessed as going to increase from FY2023 due to the impact of the workplace environment.	↑
	19	Leakage of critical corporate information, third-party confidential information, and personal information.	Assessed as greater than FY2023 due to recognition of the scope of impact.	↑
	20	Business suspension due to improper license and approval.	The degree of impact, including certification, is assessed as going to increase.	↑
	21	Difficulty to collect sales receivables, loan loss.	Assessed as being at a level similar to FY2023.	—
	22	Impairment of assets.	Assessed as being at a level similar to FY2023.	—
	Climate change risks	1	Increase in raw material costs.	Assessed as high-risk due to the direct impact on manufacturing and procurement costs, and the possibility of being unable to procure parts due to induced cost increases.
2		Increasing environmental awareness of customers and investors.	The short to medium-term risk is low, but the probability of occurrence is higher than FY2023.	↑
3		Delay relative to competitors in the transition of existing and new products to low-emission / low-carbon technologies.	Lags in eco-friendly technology were assessed as leading to future business risks.	—
4		Trends in carbon pricing.	It is assessed that the impact of regulations and legal systems will increase due to the growing global movement toward reduction of CO ₂ emissions.	↓
5		Natural disasters.	While temperature fluctuations could lead to various risks such as natural disasters, this was assessed as having a lower probability in the short to medium-term.	↓