Materiality Initiatives

Build a risk management system

Materiality

- All risks disclosed on the securities reports are evaluated by the department in charge, and the risks to be addressed in priority are identified
- Reduce the impact of the risks to be addressed in priority on our business Manage the progress of reducing such impact and the residual risks

Corporate Governance

Background to the identification of materiality

If the department responsible for appropriately managing risks is not identified, or if risk assessments are not carried out and risks that should be dealt with as a priority are not identified, it will be impossible to take appropriate action in the event of unexpected circumstances, and there is a possibility that this could have a serious impact on the business. The NIDEC Group is working to ensure business continuity by taking a global perspective and looking at both medium- to long-term risks and day - to - day risks that could affect the business. To this end, we have established a system for investigating and evaluating risk events while confirming the effectiveness of current countermeasures.

Initiatives in FY2023

We carefully examined whether the risk events that each department in charge of risk management is evaluating reflect changes in the internal and external business environment and customer requests. We also narrowed down the risk events to be evaluated in order to reduce the workload of risk evaluators.

Toward the future

In addition to regular monitoring of the Key Risk Indicators (KRI) established for the major risks identified in the risk assessment, we will also report on the issues and countermeasures for individual matters at the Board of Directors' Meeting and Executive Management Meeting, and verify the effectiveness of risk management activities across the entire NIDEC Group.

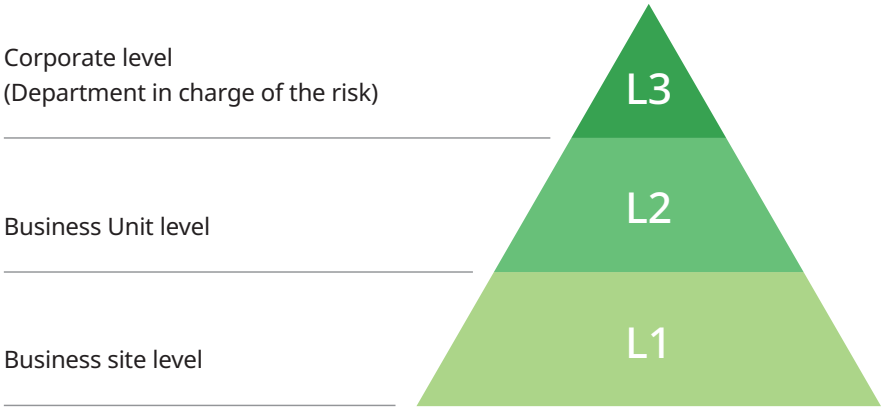
Risk Investigation and Assessment Activities

At each of the levels shown in Figure 1, the general manager of the business site, the general manager of the department, and other persons designated by the Risk Management Committee, which is an advisory body for risk management in the NIDEC Group, regularly investigate and assess risk events that could affect business operations. The risk events to be investigated and assessed are broadly classified into the following four categories.

- **Management strategy risk**
- **Business operation risk**
- **Governance risk**
- **Contingency risk**

When investigating and evaluating risks, we check the current status of risk management activities and risk reduction measures, monitor residual risks, and use the results in measures at other levels. For example, we are promoting the inter-relationship of tiered risk management activities, such as checking the content of risks identified at L2 at L3, and if we find issues that must be improved across the entire group, we will reflect them in L3 risk management activities as appropriate.

Risk Investigation and Assessment Activities (Figure 1)



L = Level

List of especially significant risks

Of the risk events that were evaluated at L3 in FY2023, the "especially significant risks" that are considered to have a significant impact on our business are as shown in Figure 2. For details of other business risks and countermeasures, please refer to the Annual Securities Report, 51st Term (submitted on June 19, 2024).

The risk level is the result of evaluating the likelihood of occurrence and the severity of the consequences on a scale of 1 to 5, and then applying them to the matrix in Figure 3, which is divided into four levels: serious, high, medium, and low.

Especially significant risks (Figure 2)

Risk classification	Risk details	Main countermeasures	Risk Level
1. Management strategy risks			
Risks related to political and economic downturns	Unexpected economic fluctuations or stagnation in the countries or regions where our products are produced or consumed, or deterioration in political or policy trends	• Reduce risks and maximize business opportunities by promoting the opening of business sites (local sales and development activities) and local production for local consumption (local production and sales activities) • Reduce dependence on business models of existing businesses through timely confirmation and review of the business portfolio, and promote business and organizational renewal for sustainable corporate growth	High
Risks related to changes in the technological environment and industrial structure	Changes in demand against the backdrop of technological change, and changes in customer trends that exceed our expectations	• Accelerate business portfolio conversion, such as concentrating resources on new products	High
Risks related to competition	• Changes in the market environment, such as the maturation of existing markets and the obsolescence of technology • Changes in competitive relationships, such as intensifying competition, new entries by other companies, and changes in competitors' strategies	• Maintain and increase investments in R&D fields, and expand manufacturing, sales and marketing capabilities • Timely launch of new products • Further improve profitability of existing products • Reduce costs to ensure profitability	High
Risks related to prior investments for anticipated customer demands	• Obsolescence of equipment due to technological innovation, excess inventory, and excess labor • Insufficient CAPEX due to underestimation of demand	• Consider thoroughly the necessity, recoverability, and amount of investment in the process of deciding on capital investment • Confirm progress against the plan monthly and consider appropriate measures/minimize loss risk • Minimize damage to economic value due to obsolescence • Reduce financial risk by minimizing the amount of investment	High
Risks related to M&A	• Deterioration in the performance of acquired businesses, loss of key personnel • Damage caused by inadequate prior investigation (due diligence)	• Select companies to be acquired in line with NIDEC's business strategy • Purchase at a reasonable price following thorough preliminary investigation • Prompt and thorough post-acquisition PMI • Increase the corporate value of the acquired company and minimize the risk of goodwill impairment while deeply instilling NIDEC's management philosophy and management methods in all employees and creating synergies upon entering the Group	Serious
2. Business operation risks			
Risks related to recruiting and retaining highly skilled personnel	Lack of human resources with high levels of knowledge and skills for new markets	• Gradually introduce three human resources system reforms (evaluation system, grading system, and compensation system) • Hire highly specialized human resources, secure management personnel, and strengthen development processes	Medium

Risk Level Identification Matrix (Figure 3)

Severity of the consequences	Likelihood of occurrence: 5 (At least once a year)	4 (At least once every three years)	3 (At least once every five years)	2 (At least once every ten years)	1 (At least once every thirty years)
5 (A major problem that could threaten the continuation of the business)	Serious	Serious	Serious	Serious	High
4 (A wide-ranging or long-term impact on business activities)	Serious	Serious	Serious	High	Medium
3 (Either a wide-ranging or long-term impact on business activities)	Serious	High	High	Medium	Low
2 (A limited and short-term impact on business activities)	High	High	Medium	Low	Low
1 (To the extent there is almost no impact on business activities, or to the extent that it can be resolved immediately)	Medium	Medium	Low	Low	Low

Promote information security measures

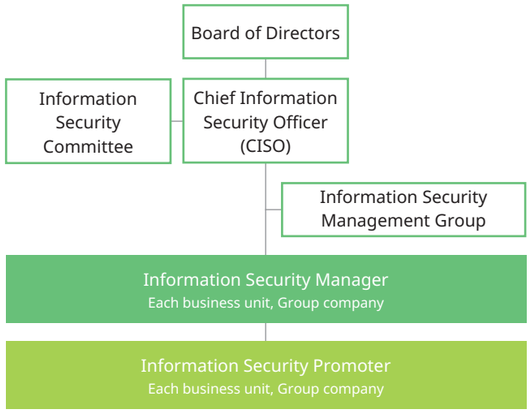
Materiality
- **Reduce the number of serious information security incidents to zero**

Corporate Governance

Background to the identification of materiality

The NIDEC Group possesses information necessary for conducting business activities, including information generated and collected by the company itself as well as information received from business partners and other sources. For this reason, we recognize the importance of appropriately protecting and using these information assets. The information we protect includes management information, technical information, financial information, and personal information, all of which are of great importance. If any of this information is damaged or leaked, we will lose the trust of our customers and the market, our competitive advantage will decline, and we may also be subject to legal penalties. We will work to prevent serious security incidents from occurring by identifying and evaluating the changing and increasing information security risks and taking effective measures in response to those risks.

Information security structure



Initiatives in FY2023

In addition to our existing efforts to prepare for external threats such as cyber attacks, we also took steps to address "Insider Threat". One of the causes of information leaks from within the company is "negligence" on the part of employees, who are careless or disregard internal rules. In order to prevent information leaks caused by this, we repeatedly conducted education and awareness-raising activities that included the seriousness of the consequences of carelessness and actions that deviate from the rules, and worked to ensure that they were understood. We also worked to introduce a system to deter and detect malicious acts by internal parties. In FY2023, there were no major accidents caused by cyber attacks or other incidents.

Toward the future

Based on the cyber attacks experienced in FY2024, the NIDEC Group will work to achieve and continuously improve high-level and uniform information security measures throughout the entire NIDEC Group under the direction of the Information Security Committee, which is constituted by NIDEC Group executives.

Strengthening physical security

Unlike cyber space, where offices are connected by networks, physical security measures such as locking, authentication, monitoring and recording have been implemented at each office to ensure that only authorized personnel can enter the relevant section, depending on the level of confidentiality. However, by establishing standard guidelines for the NIDEC Group, we will be able to ensure uniform security at all of our business sites.

Incident Response

In the case of an information security incident occurring within the NIDEC Group, we will establish standards for setting up an emergency response team, the organizations that will participate in the team, the roles of the team leaders, and the items and procedures that should be addressed, and we will develop these as standards for the NIDEC Group. We will also verify the practicality and effectiveness of the content described by conducting exercises and training in accordance with the established procedures. Through these activities, the NIDEC Group will be able to respond to emergencies in a uniform, comprehensive and timely manner.

We will continue to make improvements to achieve appropriate information security management that supports the business of the entire NIDEC Group by gradually standardizing the countermeasures that have been implemented by each company in the Group to date.