Materiality 12

Strengthening Risk Management

Reason for Prioritization

Risk management, which involves accurately identifying risks and taking proactive measures to minimize their impact, is becoming increasingly important as the risks surrounding companies, including increasing geopolitical risks, digital transformation, and climate change, become more diverse.
In addition, necessary preparations and arrangements for contingencies such as pandemics, large-scale disasters such as an earthquake directly under the Tokyo metropolitan area or a massive Nankai megathrust earthquake, or international conflicts and wars, can help minimize damage and reduce risks.
Identifying various changing risks from a medium- to long-term perspective, and establishing countermeasures based on the resulting impacts to the economy, environment, and society, will lead to sustainable corporate growth.

Commitment

The risks facing companies are growing more diverse and complex due to the rapid evolution of technology and changes in the global socioeconomic situation. Failure to respond to such risks appropriately could result in the loss of trust among stakeholders such as customers and shareholders and may lead to damages that affect the continuity of a company. For this reason, the development of an effective risk management system is becoming increasingly more important.
The Nikon Group conducts risk assessments every year, identifies important company-wide risks, analyzes and evaluates these risks, and regularly monitors its own responses. In addition, to further enhance the effectiveness of risk response as a group, we have strengthened our internal control promotion system and formulated Nikon Global Operating Standard that summarize management directives for day-to-day operations to ensure sound and efficient management of business activities. We will use those Nikon Global Operating Standard to establish an internal control improvement process. Furthermore, we continue to develop a highly efficient and flexible Group governance system in order to improve our ability to respond to global risks, while taking into account changes in management environments and business structures.

Takumi Odajima
Representative Director and Executive Vice President
CRO, General Manager of Group Governance & Administration Division
* CRO: Chief Risk Management Officer

【Activity Policies】

- Nikon Group Information Security Policy
- Nikon Group Personal Information Protection Policy

【Organizations】

- Risk Management Committee
- Quality Committee
- Export Control Committee
- Compliance Committee

Fiscal Year 2022 Materiality Goals and Results

Self-evaluation ○: Achieved △: Measures started but not yet achieved

Goals for Fiscal Year 2030	What Nikon Needs to Do	Related SDGs	Scope	Goals for Fiscal Year 2022	Results for Fiscal Year 2022	Self-Evaluation
Identification of current and future risks and impacts, and utilization of the PDCA cycle to enhance and improve systems	Perform risk assessment and give instructions to make improvements in relation to highrisk items	–	Nikon Group	Risk identification surveys. Sharing and understanding of risk awareness throughout the company, including the head office management and audit departments	Conducted a risk identification survey, compiled measures to strengthen responses to major risks, and reported to the Risk Management Committee held in March 2023	○
Avoidance of financial loss or damage to the company's reputation through the sound operation and management of IT infrastructure and the implementation of cybersecurity and personal data protection measures	Strengthen the information security system (including cybersecurity and personal data protection)		Nikon Group	Strengthen information security (cybersecurity, personal information protection) systems and continuously comply with applicable laws and regulations in each country.	Progressed as planned with measures to make the Nikon Group global network environment more secure In addition, we took necessary measures to comply with the applicable personal information protection laws and regulations of each country	○

Risk Management

Basic Approach

The Nikon Group has implemented a risk management system in order to deal appropriately with all risks that may have a significant impact on corporate management with the aim of sustainable growth for Nikon and Group companies.

System

To properly respond to risks that might critically impact corporate management, the Nikon Group has set up the Risk Management Committee. The Committee is chaired by the Representative Director and CRO and made up of Executive Committee members, with the Administration Department and Planning Section of Group Governance & Administration Division serving as Secretariats. For the fiscal year 2022, the committee met twice, once in October 2022, and again in March 2023.

In order to respond more effectively to major risks, we have established a system that enables continuous monitoring and flexible support for priority target risks. In fiscal year 2023, we plan to strengthen risk management by establishing processes to improve internal controls, developing an export control system, and reviewing BCM.

The Risk Management Committee has jurisdiction over all risks, but three committees under the Risk Management Committee; the Quality Committee, the Export Review Committee, and the Compliance Committee, are responsible for handling risks that require specialized measures. From a sustainability perspective, the Sustainability Committee also monitors risks with a focus on materialities and addresses risks related to the environment and social and labor.

Main Activity Themes of the Risk Management Committee in the Fiscal Year 2022

- Progress & challenges for key companies to be monitored
- Internal control-related (establishment of internal control promotion system, formulation of management standards)
- Conduct company-wide risk identification survey for fiscal year 2022
- Report on results of litigation survey
- Information security compliance with personal information protection laws in various countries

Main Specialist Committees Involved in Risk Management

Committees	Principal Risks
Risk Management Committee	Risks
Quality Committee*	Quality
Export Control Committee*	Prevention of the Foreign Exchange Law Violations and Security Risk Management
Compliance Committee*	Compliance
Sustainability Committee	Sustainability in general, especially environmental (climate change, chemical management, water, etc.), social and labor (human rights, etc.)
Bioethics Review Committee	Bioethics

*Committees under the Risk Management Committee

Risk Assessment

The Nikon Group conducts risk identification surveys to gain overall insight into the risks affecting the Group, including risks such as regional conflicts and infectious diseases.
The survey results are reported to the Risk Management Committee after being compiled into a risk map presenting the scale of impacts and probability of occurrence. This survey is administered to Nikon's general managers and above, as well as presidents of Group companies in and outside Japan.
In fiscal year 2022, the risk classifications used in the Risk Identification Survey Questionnaire were substantially revised in line with the major risks from current economic, social, and environmental perspectives.
We will work with related divisions to develop a risk management system to mitigate risks such as logistics disruptions and supply chain disruptions caused by new coronavirus infections and Russia's invasion of Ukraine, as well as geopolitical risks such as the U.S.-China confrontation.

Related Information

Financial statements contain additional information about business activity and other risks within analysis of management performance and financial conditions.

Web Consolidated Financial Results (for the Year Ended March 31, 2023, P9 to P11)
https://www.nikon.com/company/ir/ir_library/result/pdf/2023/23_4qf_c_e.pdf

Climate Change Risks Faced by the Nikon Group (➡ p.073)

BCM*1 Activities Measures

The Nikon Group has formulated BCPs*2 in preparation for large-scale disasters and other emergencies, including pandemics, and reviews them every year.
In the aftermath of Russia's invasion of Ukraine in February 2022, we conducted periodic situation checks with relevant departments, particularly the Production Technology Division and business units, to prepare for subsequent contingency measures.
In response to the COVID-19 pandemic, the Company made efforts to continue business activities while utilizing telecommuting and remote work and taking company-wide infection prevention measures.
The Nikon Group in Japan reviewed its emergency communication tools and conducted various drills, including communication drills that simulate disasters, in preparation for large-scale earthquakes such as one occurring directly under the Tokyo metropolitan area or a Nankai Megathrust Earthquake, both which are assumed to have a high probability of occurrence. We also conducted drills dealing with newly intensified natural disasters such as typhoons and floods.

*1 Business Continuity Management (BCM)
Management activities carried out in normal times, such as the formulation, updating and maintenance of the BCP, implementation of proactive measures, education and training, checking and continual improvement.
*2 Business Continuity Plan (BCP)
A plan describing the policy, systems, and procedures, etc., by which corporations can avoid suspension of critical business activities, or can restore critical business quickly if it is interrupted, even when unforeseen contingencies arise, including natural disasters such as major earthquakes, pandemics, etc.

Risk Management for Information Assets and Cybersecurity

Information Assets Management Policy

At the Nikon Group, the management and security of information assets is conducted in accordance with the Nikon Group Information Security Policy. The Nikon Group Information Management Rules and other internal rules have been established based on the Policy, to ensure optimal and efficient business conduct while properly protecting information assets according to the circumstances in each country and region. These rules are posted on the internal portal site for employees to access anytime.

Web Nikon Group Information Security Policy
https://www.nikon.com/company/sustainability/governance/risk-management/security_policy.pdf

Information Management System

The Nikon Group has appointed the Representative Director and President as the head of information management, including personal information protection. We have also established operating processes in accordance with Information Security Management Systems (ISMS). In terms of systems operations, under the leadership of the Representative Director and Officer in charge of information security, the Information Security Department carries out management and supervision of activities across the entire Nikon Group. This includes formulating measures regarding information security, including responses to cyberattacks, as well as developing and maintaining systems.
In addition, the head of each organization of Nikon's business units, divisions, and the Group companies is designated as information managers. By working with the Information Security Department, these individuals are helping to build an information security management system compatible with the situation in each country and region, while comprehensively managing the entire Nikon Group. Material matters involving information asset risks are reviewed by the Risk Management Committee, which includes members of the Executive Committee and others.
Nikon's healthcare business unit has obtained ISO 27001 certification, an internationally recognized standard for ISMS (information security management system), for its research and development of computational pathology and AI assisted medical diagnosis, which requires particularly strict information management.

* ISMS: Information Security Management System

Response to Information Security Incidents

When an information security incident occurs at the Nikon Group, the site where the incident occurred is obligated to report it immediately to the Information Security Department. The Information Security Department works with relevant departments to establish a system and procedures for minimizing damage and impact, and processes for promptly resuming business. Serious cases are promptly reported to the director in charge by the Information Security Department. In addition, members of the Information Security Department participated in a training course on incident response conducted by outside experts.
There have been no major information security incidents involving the payment of fines or compensation in the past three years.

Information Security Education

The Nikon Group conducts information security e-learning education programs as part of new employee training, etc., in order to raise employee awareness and improve the effectiveness of information security. Within this education program, we include not only information about the policies and rules related to information management, but also provide specific examples as well.
In addition, the Nikon Group Information Security Handbook, an educational document that provides easy-to-understand explanations of the information security measures that are disseminated through internal regulations and bulletins, is posted on the portal site for all employees to refer to at any time. This handbook is used in regular training to make sure that every one of the employees understands the importance of information asset management and complies with the rules with strong awareness.
In the fiscal year 2022, as in previous years, we designated February as Information Security Awareness Month, raising awareness through in-house newsletters and conducting an e-learning program for domestic Group companies. Furthermore, we conducted orientation training for employees hired regularly, which involved lectures and sessions facilitated by instructors. Group companies outside Japan also conducted information security education through e-learning or other methods as appropriate.
Through these training programs, we ensure that our employees are thoroughly familiar with information security. In the unlikely event that an employee violates the relevant rules and causes an incident such as information leakage, the employee may be subject to disciplinary action in accordance with the employment rules of the company to which the employee belongs.

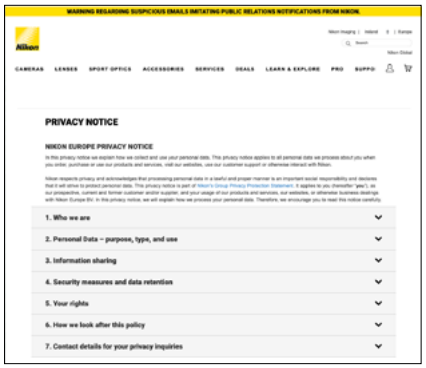
Information Security Audit

The Nikon Group periodically conducts internal audits pursuant to the Nikon Group Information Management Rules to improve the level of our information security.
In the fiscal year 2022, a paper-based audit was conducted on all of the Nikon Group's organizations (Nikon business departments and Group companies) in Japan and onsite audits were carried out on selected organizations based on materiality themes. The results of these audits indicate there were no significant risks. The Nikon Group plans to conduct internal audits focusing on the presence of appropriate information security measures in the fiscal year 2023.

Personal Information Protection

The Nikon Group has established the Nikon Group Privacy Protection Statement based on its respect for privacy and acknowledgment that processing personal data in a lawful and proper manner is an important social responsibility. Additionally, under this Statement, we established the Nikon Group Personal Data Processing Rules as a common set of rules covering the entire Group. We are now working to make these rules known within the Group and ensuring that personal data is handled in accordance with these rules under the information management system.
Furthermore, we established the Personal Data Protection Subcommittee under the Risk Management Committee comprised of members from the Executive Committee and other organizations. The subcommittee carries out risk management concerning privacy and personal information covering the entire Nikon Group.
Our specific initiatives include posting privacy notices on the website of each Nikon Group company in accordance with relevant laws and regulations, and notifying customers of contact information for support regarding privacy and individual rights. This includes the purpose of use of personal information and how to delete their personal information.
In addition, we request that procurement partners follow the Nikon CSR Procurement Standards in order to maintain information security, including privacy protection.

Web Nikon Group Privacy Protection Statement
https://www.nikon.com/privacy/group/
Privacy Notice of Nikon Europe B.V. in accordance with the EU General Data Protection Regulation (GDPR)
https://www.nikon.ie/en_IE/footers/privacy_policy.page
Nikon CSR Procurement Standards
https://www.nikon.com/company/corporate/procurement/csr/



Privacy Notice of Nikon Europe B.V. in accordance with the EU General Data Protection Regulation (GDPR) (excerpt)

Response to the Personal Information Protection Laws of Each Country

The Nikon Group complies with the personal information protection laws of each country where it operates, including the General Data Protection Regulation (GDPR) in the EU. We are also working to develop a system to prevent violations in order to achieve appropriate management of personal information under an information security management system.

In fiscal year 2022, we promoted compliance with Thailand's Personal Data Protection Act, posted privacy notices at group companies in Thailand, and took other necessary actions. With regard to the U.S., we have reviewed our privacy policy in accordance with the California Consumer Privacy Act. We continuously collect information on legislation and revision trends of personal information protection-related laws and regulations in other countries and regions. In addition, seminars on the Act on the Protection of Personal Information were held to promote employee awareness.
In fiscal year 2023, we will continue to take necessary actions in line with the enactment or revision of personal information protection-related laws and regulations in each country and region.

Cybersecurity Infrastructure Development and Process Improvement

In order to maintain a high level of defense against increasingly sophisticated and stealthy cyberattacks, the Nikon Group is improving and strengthening its operational system to collectively monitor and respond to cyberattacks on a global basis. This includes enhancing early detection and early response capabilities. We are also in the process of deploying a system to filter out phishing scams and other suspicious e-mails.
Furthermore, we continue to regularly improve our existing operating processes. For example, we conduct periodic checks on the vulnerability of our corporate website, which could become an entry point for cyberattacks. We regularly conduct training for designers on information security rules during the product development process.