

Strengthening Risk Management

Reason for Priority

Risk management involves properly identifying risks and implementing measures in advance to minimize the impacts of those risks. The importance of risk management is growing amid the diversification of risks facing companies due to advancements in IT and AI technologies, the globalization of business, and environmental issues such as climate change.

In addition, making the necessary preparations and arrangements before a major disaster, such as the COVID-19 pandemic, a Greater Tokyo Area earthquake, or the Nankai megathrust earthquake, will help prevent damage and reduce risk.

Taking measures to identify, from a medium- to long-term perspective, various changing risks and thus mitigating impacts on business, the environment, and society represents one path to achieving sustainable development.

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 order for the Group to further increase the effectiveness of risk response going forward, we are focusing on improving the internal control promotion system and the functionality of three lines of defense (first line: business departments; second line: corporate administration departments; and third line: internal audit departments) and strengthening mutual collaboration. Furthermore, we continue to develop a highly efficient and flexible Group governance system in order to improve our responses to global risks, while taking into account changes in management environments and business activity structures.

Takumi Odajima
Representative Director and Executive Vice President
CRO, General Manager of Group Governance & Administration Division

* CRO: Chief Risk Management Officer

[Policy for Activities]

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

[System]

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

Goals for the fiscal year ending March 2031 (What Nikon Intends to Achieve)	What Nikon Needs to Do	Related SDGs	Goals for the fiscal year ended March 2022	Scope	Results
<p>Identification of current and future risks and impacts, and utilization of the PDCA cycle to enhance and improve systems</p> <p>Avoidance of financial loss or damage to the company's reputation through the sound operation and management of IT infrastructure and the implementation of group cybersecurity and data protection measures</p>	<p>Perform risk assessment and give instructions to make improvements in relation to high-risk items</p>	<p>—</p>	<p>Implement risk reduction through strengthening of coordination between the major related departments and through a new, company-wide risk management system</p>	<p>Nikon Group</p>	<p>Group governance initiatives have been initiated, and a certain level of results has been achieved in improving departments and organizations with high internal control risks. Monitoring is scheduled to continue in the next fiscal year to confirm adherence.</p>
	<p>Strengthen the information security system (including cybersecurity and personal data protection)</p>		<p>Review the framework for monitoring emerging risks</p>	<p>Nikon Group</p>	<p>Discussions held among risk management-related divisions to develop a system for identifying emerging risks in the future</p>
	<p>Put in place a system for preventing violations that are accompanied by fines, in response to the 2020 amendments to Japan's Personal Information Protection Act</p> <p>Continuously review the EU General Data Protection Regulation (GDPR)</p>		<p>Nikon Group</p>	<p>No regulatory violations that were accompanied by fines. The revised Personal Information Protection Law was addressed as planned, with revisions made to the contents of notices regarding personal information protection and related regulations within the Group. We conducted another GDPR checklist for each company and confirmed that they were compliant with the law.</p>	

Risk Management

Basic Approach

Approach and Policy

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

Framework and 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 ended March 2022, the committee met twice, once in October 2021, and again in March 2022.

In order to respond more effectively to major risks, a subcommittee has been established within the Risk Management Committee to provide ongoing monitoring and flexible support for priority risks. In the fiscal year ending March 2023, we plan to further strengthen cooperation between related divisions to reduce risk through the promotion of internal controls and an enterprise risk management system. The Risk Management Committee has jurisdiction over all risks, but the Quality Committee, Export Control Committee, and Compliance Committee have been established under this committee, and each specialized committee works on detailed responses to risks that require specialized action.

Main Activity Themes of the Risk Management Committee in the fiscal year ended March 2022

- Progress & challenges for key companies to be monitored
- Ongoing monitoring of internal audit results
- Conduct company-wide risk identification survey for fiscal 2021
- 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	Comprehensive CSR and environmental issues (climate change, management of chemical substances, water, etc.)
Bioethics Review Committee	Bioethics

*Committees under the Risk Management Committee

Risk Assessment

The Nikon Group conducts risk identification surveys to gain an overall insight into the risks affecting the Group, including new 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 the fiscal year ended March 2022, we identified principal companies to be monitored and risk management cases on which to focus and worked to address and improve them. In addition, we increased collaboration between the Risk Management Committee, Internal Audit Department and Corporate Administration Department in an effort to further develop our risk management system and mitigate risks.

Related Information

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



Consolidated Financial Results for the Year Ended March 31, 2022 (P9 to P10)
https://www.nikon.com/about/ir/ir_library/result/pdf/2022/22_4qf_c_e.pdf

BCM*¹ Activities Measures Activities and Results

The Nikon Group has formulated BCPs*² in preparation for large-scale disasters and other emergencies, including pandemics, and reviews them every year.

In response to the spread of the COVID-19 pandemic, we worked to ensure that each employee was aware of and thoroughly applied infection prevention measures. We were also able to continue our business activities while taking infection prevention into consideration by promoting telecommuting and other measures.

Due to the increased probability of the occurrence of a large-scale earthquake such as a Greater Tokyo Area earthquake or the Nankai megathrust earthquake, as well as the occurrence of intensified natural disasters, including typhoons and floods, in recent years, the Nikon Group in Japan carried out communication training based on the scenario of communicating during an emergency, and training to confirm communication methods using satellite phones, at the same time disaster training was held at its production bases.

*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

Approach and 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.

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

Information Management System

System and Framework

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

Activities and Results

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, when appropriate, members of the Information Security Department attend incident response training courses run 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

Activities and Results

The Nikon Group is working to both raise awareness among employees and increase the effectiveness of its information security. Specifically, in addition to new hire orientation training, we provide education on information security regularly using e-learning and other methods. Within this education program, we include not only information about the policies and rules related to information management, but 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 ended March 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. Group companies outside Japan also conducted information security education through e-learning or other methods as appropriate. Preparations were also made to update the content of the new employee orientation training from April 2022.

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

Activities and Results

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 ended March 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 ending March 2023.

Personal Information Protection

Approach and Policy

System and Framework

Activities and Results

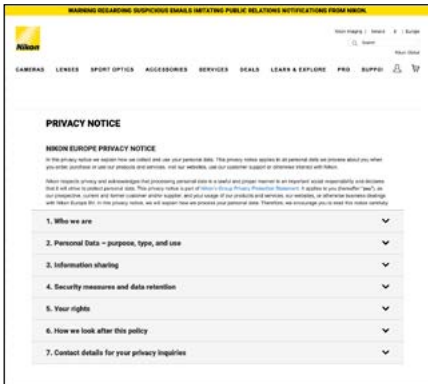
The Nikon Group has established the Nikon Group Privacy Protection Statement based on its respect for privacy and acknowledgment that processing personal data in a lawful and proper manner is an important social responsibility. Additionally, under this Statement, we established the Nikon Group Personal 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 security promotion 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, the subcommittee requests that procurement partners follow the Nikon CSR Procurement Standards in order to maintain information security, including privacy protection.



- Nikon Group Privacy Protection Statement
https://www.nikon.com/privacy/privacy_policy.htm
- 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/about/corporate/procurement/pdf/csr-procurement1_3_e.pdf



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 the fiscal year ended March 2022, we took measures to comply with the Amended Act on Protection of Personal Information that will take effect on April 1, 2022. In addition, we continued to collect information on the Personal Data Protection Act of the Kingdom of Thailand, the enforcement of which has been postponed, and legislative and revision trends concerning personal information protection-related laws and regulations in other countries and regions.

In the fiscal year ending March 2023, we will continue

to respond to the implementation of the Personal Data Protection Act in Thailand, as well as to the California Privacy Rights Act in the United States, which will take effect in January 2023.

Cybersecurity Infrastructure Development and Process Improvement

Activities and Results

To maintain a strong defense against increasingly sophisticated and stealthy cyberattacks, the Nikon Group continued to deploy cybersecurity measures that were first introduced during the fiscal year ended March 2021. We also strengthened our operational system to collectively monitor and respond to cyber-attacks globally in order to achieve early detection and early response. We are also in the process of updating our system to filter out phishing scams and other suspicious e-mails. In response to the increased number of telecommuting opportunities under the “new normal” we are developing an IT infrastructure that can be accessed securely from anywhere outside the company through the use of cloud technology and other means.

In addition, we regularly improve our conventional 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.