Contents/Editorial Policy | Message from the President | Nikon Group Profile | Nikon's Sustainability | Business Activity | Environment | Society/Labor | **Governance** | Corporate Citizenship Activities

> Thorough Compliance   > Strengthening Corporate Governance   **> Strengthening Risk Management**

Materiality 12

Strengthening Risk Management

The Nikon Group implements both offensive and defensive risk management by identifying material risks that could impair corporate value, taking proactive risks to support the sustainable growth of Nikon and our Group companies, and taking appropriate preliminary actions to prevent fraud, accidents, and other issues.

Activity Policies

■ Nikon Group Information Security Policy
■ Nikon Group Privacy Protection Statement
■ Basic Policy on Internal Control System

Organizations

■ Risk and Compliance Committee
■ Export Control Committee

● Indicators and Targets

Self-Evaluation   ○：Achieved   △：Measures partially achieved or revised

Indicators	Targets (Year of Achievement)	Fiscal Year 2024 Plan (Action Plan)	Fiscal Year 2024 Results	Self-Evaluation	Fiscal Year 2025 Plan (Action Plan)
Progress in identifying important risks and implementing measures based on risk assessments	100% (every fiscal year)	• Support the optimization of export control systems in Group companies • Implement measures to improve the effectiveness of BCP for large-scale disasters and BCM for international conflict contingencies (familiarization and training, continuous updates)	• Established export management and service management systems for newly added (M&A) Group companies outside Japan; enhanced cooperation with business units overseeing these new members • Conducted a response drill in January 2025 simulating a major disaster. The IT Solutions Division began discussions with the Production Technology Division (Group production company) on BCM collaboration	○	• Redesign and implement a risk assessment framework • Identify critical risks and consider policies to address these risks
		• Strengthen cybersecurity systems and comply with laws and regulations in each country that require product cybersecurity measures	• Strengthened cybersecurity systems and complied with laws and regulations in each country that require product cybersecurity measures	○	• Continue to comply with laws and regulations in each country that require product cybersecurity measures

Contents/Editorial Policy | Message from the President | Nikon Group Profile | Nikon's Sustainability | Business Activity | Environment | Society/Labor | **Governance** | Corporate Citizenship Activities

> Thorough Compliance   > Strengthening Corporate Governance   **> Strengthening Risk Management**

Risk Management

Basic Approach

Risk management covers external factors including geopolitical risks, digital transformation, and climate change, as well as internal factors including the risk of not achieving targets in the Medium-Term Management Plan. We investigate and analyze increasingly diverse corporate risks, predict their potential impact, and work to avoid, reduce, or strategically take risks to support sustainable growth.

Strategy

Risk

Our business environment is heavily influenced by external factors such as geopolitical risks, rising policy interest rates to control inflation in various countries, higher tariffs, and the weak yen. We must take appropriate measures to address risks arising from major market changes and other fluctuations in the business environment

Failure to respond to such risks appropriately could result in the loss of trust among customers, shareholders, and other stakeholders, and may lead to damages that affect the continuity of our company.

Opportunities

Risk management not only minimizes the impact of issues like fraud or accidents but also supports risk-taking as a means of executing business strategy.

Accurately identifying and prioritizing key management risks in our company in response to social and environmental changes enables business development aligned with management strategy and supports future profit generation and sustainable growth.

Strategy

The Nikon Group conducts surveys on internal and external perceptions of risk to understand the risks our Group faces. We identify our key management risks and reflect our findings in the goals and initiatives of each department and Group company.

Related Information

Our Consolidated Financial Results contains additional information about business and other risks within analysis of management performance and financial conditions.

⬀ Consolidated Financial Results for the Fiscal Year Ended March 31, 2025 (IFRS)

Governance

Risk Management Committee

To properly respond to risks that might critically impact corporate management, the Nikon Group has set up the Risk Management Committee. The committee meets twice a year and is chaired by the president and CEO, who also serves as chief risk officer (CRO). The Group Governance &

Administrative Division serves as the secretariat and committee members include members of the Executive Committee. The Risk Management Committee strives to build a framework to monitor priority risks and provide prompt response.

We integrated the Risk Management Committee and its subordinate Compliance Committee in April 2025 and renamed it the Risk and Compliance Committee. The newly constituted committee discusses compliance-related risks as part of company-wide risk management.

● **Main Agenda Items of the Fiscal Year 2024 Risk Management Committee**

October 2024	• Risk assessments for key proposals submitted to the Executive Committee
March 2025	• Risk assessments for key proposals submitted to the Executive Committee • Integration of the Risk Management Committee and Compliance Committee to strengthen company-wide risk management (re-launched as the Risk and Compliance Committee on April 1, 2025) • Revised the escalation process to strengthen crisis response

Risk Management Framework

The Nikon Group implements our risk management framework through three lines of defense. These lines consist of business divisions, administrative divisions, and internal audit divisions, respectively. Our first line of defense establishes various regulations and report lines, creating an autonomous risk control system that also covers relevant Group companies. The second line of defense supports the first line in risk control and assessment, respectively.

| Contents/Editorial Policy | Message from the President | Nikon Group Profile | Nikon's Sustainability | Business Activity | Environment | Society/Labor | **Governance** | Corporate Citizenship Activities |

> Thorough Compliance   > Strengthening Corporate Governance   **> Strengthening Risk Management**

Our third line of defense conducts objective audits, independent of business execution divisions, evaluates if internal controls of the first and second lines are functioning, and gives advice.

Cooperation with Related Committees

While the Risk Management Committee has jurisdiction over all risks, the committee works in coordination with subordinate committees, the Sustainability Committee, and other relevant committees and subcommittees to address risk that require specialized responses.

● Main Specialist Committees Involved in Risk Management (Since April 2025)

Committees	Principal Risks
Risk and Compliance Committee	General risks and compliance
Quality Committee	Quality
Export Control Committee *	Prevention of foreign exchange law violations and security risk management
Sustainability Committee	Sustainability in general, especially environmental (climate change, chemical management, water, etc.), social and labor (human rights, etc.)
Bioethics Review Committee	Bioethics

＊ Subordinate committee of the Risk and Compliance Committee

Risk Management

The Nikon Group conducts a risk identification survey each year to assess and understand risks facing the Group. We conduct this survey with Nikon department managers and presidents of Group companies in and outside Japan to identify, analyze, and evaluate company-wide key risks and monitor response status. We then analyze risk identification surveys with high response volume or significant impact based on the results and incorporate external perspectives to create a risk correlation map and identify key risks. The Risk and Compliance Committee determines which issues require stronger action.

The Risk and Compliance Committee identifies top-priority risks that require specialized responses from a management perspective based on information from the Sustainability Committee, the Quality Committee, and the Export Control Committee, a subordinate committee under the Risk and Compliance Committee. The Risk and Compliance Committee issues directions for action and manages progress of these risks. The Board of Directors receives these reports and supervises Nikon Group risk and risk management overall. Internal audits conducted by the Internal Audit Department confirm the adequacy of risk management.

We will incorporate responses to identified key risks into the next Medium-Term Management Plan. Based on the measures and progress within relevant departments, we will define policies for the Risk and Compliance Committee and strengthen the risk management framework while working to mitigate risks.

Major Initiatives

Risk Management Education

The Nikon Group conducts an annual Risk Awareness Survey with Nikon department managers and presidents of Group companies in and outside Japan to raise awareness and understanding of risks.

We updated the Nikon Global Operating Standard, which serves as guidance for business units and Group companies to ensure efficient and sound operations, based on the latest conditions. We outlined 40 key items that require attention in our business activities. Each department selected priority items for fiscal year 2024 and is implementing improvement measures accordingly.

BCM[1] Activities Measures

The Nikon Group formulates and reviews BCPs[2] in preparation for large-scale disasters and other emergencies, including pandemics.

We conducted an initial response drill for a large-scale disaster in January of fiscal year 2024. Through this drill, we identified BCM issues and reflected such issues in our measures.

We will continue to optimize our BCP and update our initial response plan for international conflict contingencies.

＊1 Business Continuity Management (BCM): Typical management activities such as BCP formulation, updates, and maintenance, as well as the implementation of proactive measures, education, trainings, inspections, and continuous improvements.
＊2 Business Continuity Plan (BCP): A plan describing the policy, systems, 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.

Contents/Editorial Policy | Message from the President | Nikon Group Profile | Nikon's Sustainability | Business Activity | Environment | Society/Labor | **Governance** | Corporate Citizenship Activities

> Thorough Compliance   > Strengthening Corporate Governance   **> Strengthening Risk Management**

Export Control Initiatives

The Nikon Group engages in security export control to help maintain international peace and security. We worked in fiscal year 2024 to support the optimization of export control frameworks across Group companies in response to increasingly strict export regulations driven by economic security and geopolitical risks. Specifically, we strengthened group governance in export control by establishing export management and service management systems for companies outside Japan that became new Group companies through M&A. We also strengthened coordination among the business units that oversee these new members.

Contents/Editorial Policy | Message from the President | Nikon Group Profile | Nikon's Sustainability | Business Activity | Environment | Society/Labor | **Governance** | Corporate Citizenship Activities

> Thorough Compliance   > Strengthening Corporate Governance   **> Strengthening Risk Management**

Risk Management for Information Assets and Cybersecurity

Basic Approach

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

Strategy

Risk

Nikon may face operational disruptions and financial losses, including reduced revenue, in the event of a cyberattack that compromises our systems. Theft or leakage of confidential or personal information may also lead to reputational damage to our information management, resulting in a loss of trust in our company, and potential claims for damages.

Opportunities

Conducting proper information security measures and information asset management enables us to reduce our risk of cyberattacks. These measures help improve information availability, support business continuity, and enhance trust in the Nikon Group.

Strategy

We will strengthen trust in the Nikon Group by implementing the following initiatives over the short term to medium to long term to advance information security measures and information asset management, as well as support business continuity.

In fiscal year 2025, we will strengthen cybersecurity systems and comply with laws and regulations in each country that require product cybersecurity measures.

To achieve the targets of the current Medium-Term Management Plan, we will enhance cybersecurity and establish a global IT and security framework and governance.

We also aim to establish a company-wide risk management system aligned with environmental changes and business strategy as a part of our efforts to achieve Vision 2030.

Governance

The Nikon Group appoints the president as the head of information management, including personal information protection. We also established operating processes in accordance with Information Security Management Systems (ISMS). The Information Security Department, under the supervision of the president, manages these operating processes and oversees them across the entire Group.

In addition, the head of each organization of Nikon's business units, divisions, and Group companies are designated as information managers. By working with the Information Security Department, these individuals are establishing an information security management system compatible with the situation in each country and region, while comprehensively managing the entire Nikon Group.

The Information Security Department reports material matters involving information asset risks to the Information Security Meeting and the Risk and Compliance Committee (renamed in April 2025), which includes Executive Committee members. The department then translates the reported material matters into strategies and policies, and reports to the Information Security Meeting and the Risk Management Committee. The department also sets measurable targets for these strategies and policies and tracks performance.

＊ISMS: Information Security Management System

Healthcare Business Unit Initiatives

In the Healthcare Business, Nikon works to expand business in information services centered on digitalization, including support for network-based remote diagnosis and services that store and manage cloud-based pathology images. As business expands, we will be faced with handling more personal medical information for subjects and patients, which requires strict management at medical institutions. Given these circumstances, Nikon works to ensure thorough information security management. We not only

Contents/Editorial Policy | Message from the President | Nikon Group Profile | Nikon's Sustainability | Business Activity | Environment | Society/Labor | **Governance** | Corporate Citizenship Activities

> Thorough Compliance   > Strengthening Corporate Governance   **> Strengthening Risk Management**

increased the number of organizations subject to ISO 27001 in December 2023, but we also obtained ISO 27017 certification (a code of practice in information security management for cloud services) and launched operations.

Risk Management

The Nikon Group creates a security risk map based on risk frequency and impact, and plans and implements corresponding measures against risks. The Information Security Meeting evaluates the effectiveness of these measures and reflects the results in the plans for the following fiscal year.

Major Initiatives

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.

The department revised the documentation related to the incident response process and conducted incident response training in fiscal year 2024.

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.

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 fiscal year 2024, the Information Security Department introduced an information security education platform and conducted e-learning for Nikon and Group companies in Japan. For regular new employees, we conduct training led by instructors, and for mid-career hires, we provide e-learning programs.

The Group will introduce and deploy our information security training platform to Group companies outside Japan beginning in fiscal year 2025.

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 fiscal year 2024, a paper-based audit was conducted on all of the Nikon Group's organizations (Nikon business departments and Group companies) in Japan and on-site 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 fiscal year 2025.

Personal Information Protection

The Nikon Group has established the Nikon Group Privacy Protection Statement based on our 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 ensure 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 and Compliance Committee, comprised of members from the Executive Committee and other organizations. The subcommittee carries out risk management concerning privacy and

Contents/Editorial Policy | Message from the President | Nikon Group Profile | Nikon's Sustainability | Business Activity | Environment | Society/Labor | **Governance** | Corporate Citizenship Activities

> Thorough Compliance   > Strengthening Corporate Governance   **> Strengthening Risk Management**

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.
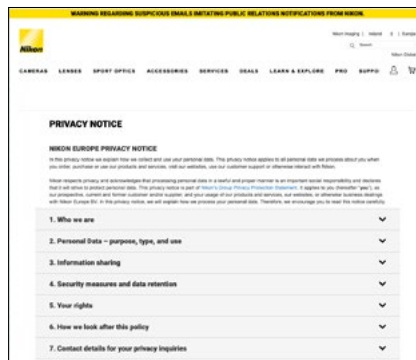
In addition, we request that procurement partners follow the Nikon CSR Procurement Standards in order to maintain information security, including privacy protection.

Web Nikon Group Privacy Protection Statement

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

Nikon CSR Procurement Standards

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 continuously monitors legislative developments related to personal data protection laws in each country and region, including the EU General Data Protection Regulation (GDPR), to ensure proper management of personal information under a robust information security system.

In fiscal year 2025, 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.

Improving Cybersecurity Infrastructure and Processes

In order to maintain a high level of defense against increasingly sophisticated and stealthy cyberattacks, the Nikon Group is improving and strengthening our operational system to collectively monitor and respond to cyberattacks on a global basis. This includes enhancing early detection and early response capabilities. We also operate a system deployed 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 also conduct training for designers on information security rules for the product development process.