Corporate Governance

Fundamental Policy

In order to establish a sound corporate governance structure and continuously raise corporate value, Canon Inc. believes that it is essential to improve management transparency and strengthen management supervising functions. At the same time, a sense of ethics and mission held by each executive and employee of a company is very important in order to achieve continuous corporate growth and development.

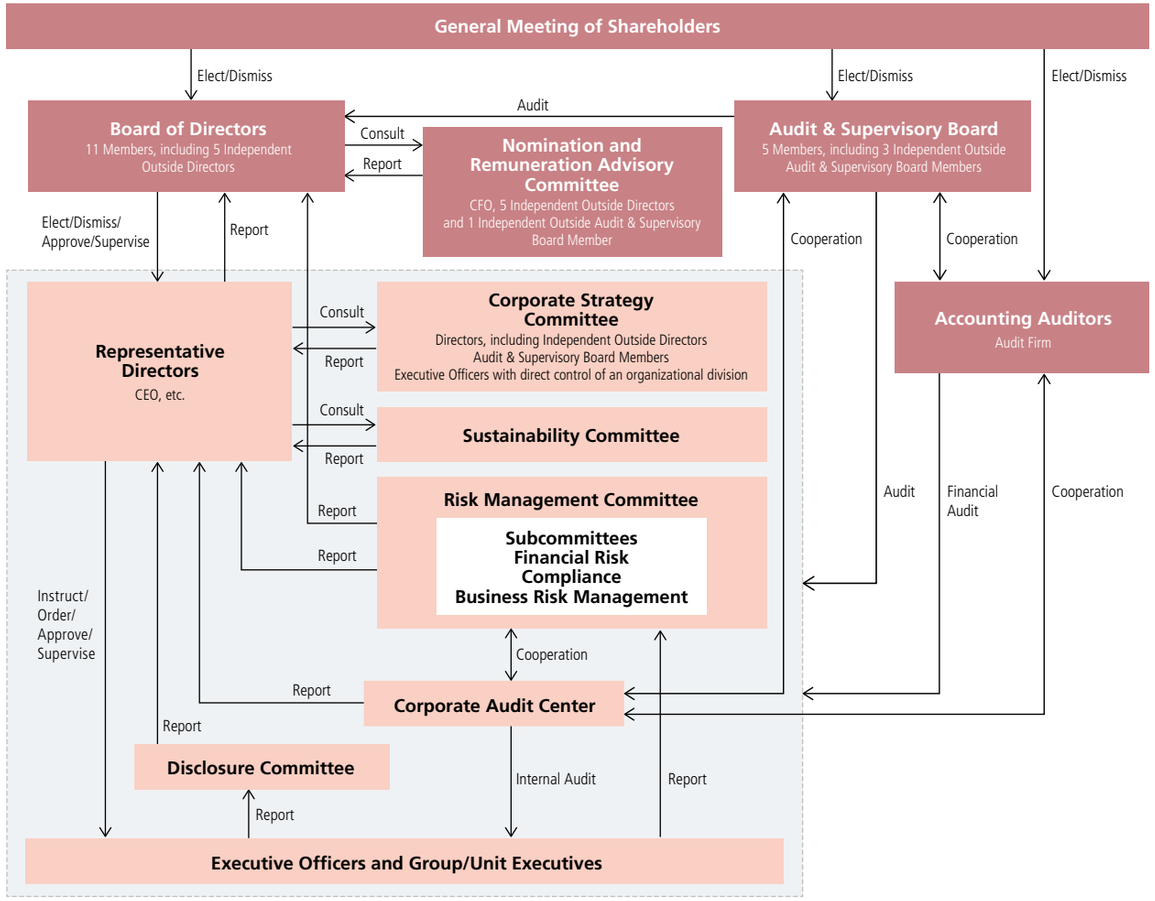
Governance Structure

Canon Inc. is globally expanding its businesses in various business fields, including printing, medical, imaging, and industrial, and aims to aggressively expand into new business fields in the future. In order to make prompt decisions in each business field, and make important decisions for the entire Canon Group or on matters that straddle several business fields from a company-wide perspective and at the same time secure appropriate decision making and execution of operation, Canon Inc. judges the corporate governance structure shown on the right to be effective.

Change in Corporate Governance Structure

2010	• Reduced the number of Directors (from 25 to 17)
2014	• Appointed Outside Directors (two)
2015	• Appointed female Executive Officer • Measures to assess effectiveness of Board of Directors
2016	• Reduced the number of Directors (from 17 to 6) • Established Nomination and Remuneration Advisory Committee • Established the Independence Standards for Independent Directors/Audit and Supervisory Board Members
2024	• Appointed a female Director • Increased the number of Directors (from 5 to10)
2025	• Appointed a female Audit & Supervisory Board Member
2026	• Increased the number of female Directors (from 1 to 2)

Corporate Governance Structure (as of April 1, 2026)



* The grey boxes represent the Organizations executing operations

For more information on corporate governance, see the following.
Reference: An Overview of Corporate Governance at Canon Inc.
https://global.canon/en/ir/strategies/governance.html
Reference: Integrated Report
https://global.canon/en/ir/library/integrated.html
Reference: Corporate Governance
https://global.canon/en/sustainability/governance/corporate-governance/

Risk Management

Basic Approach

At Canon, we recognize that to ensure proper operations and to continually improve corporate value, implementation and maintenance of a risk management system to deal with significant risks that the Group may face in business operations is vital.

Risk Management System

Canon Inc. has established a risk management committee based on a resolution of the Board of Directors. Chaired by the CFO, the committee has established three subcommittees: the Financial Risk Management Subcommittee, Compliance Subcommittee, and Business Risk Management Subcommittee.

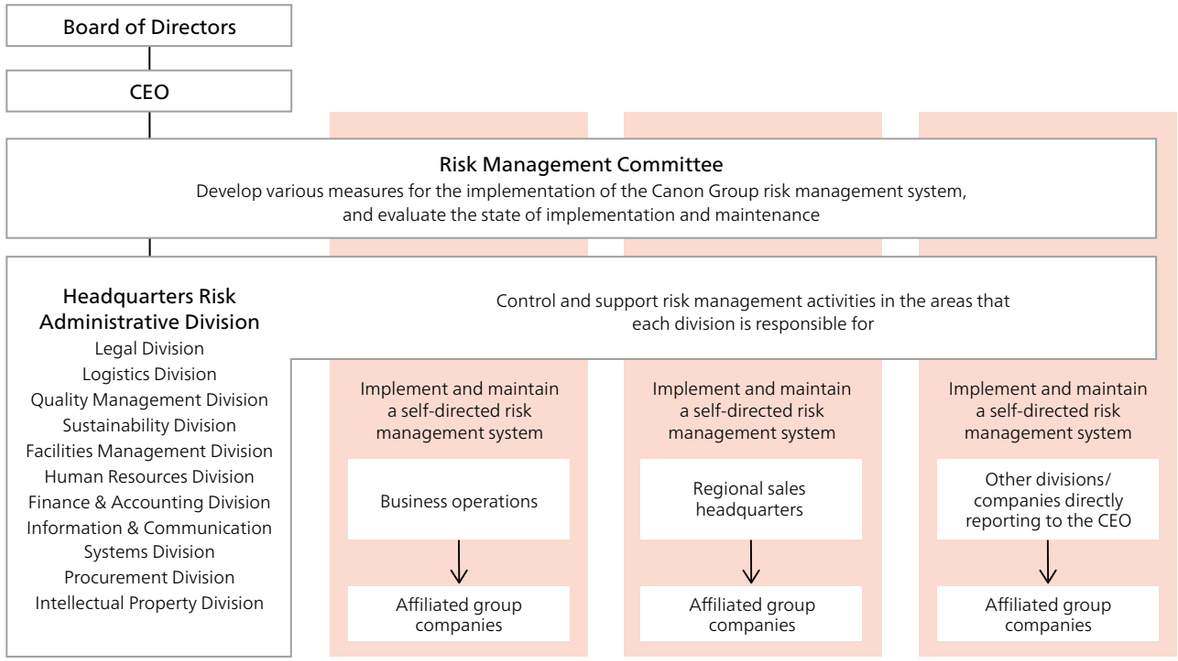
The Risk Management Committee develops various measures to implement Canon's risk management system, including identifying any significant risks (violations of laws and regulations or corporate ethics, inappropriate financial reporting, environmental issues, quality issues or information leaks, etc.) that the Group may face in the course of business.

Canon Inc. administrative divisions responsible for various risks associated with business activities, including the Legal Division, Logistics Division, Quality Management Division, Human Resources Division, Finance & Accounting Division, belong to the relevant subcommittee and according to their areas of responsibility, control and support the risk management activities of each Canon Inc. division and Group company.

Processes for Implementation and Maintenance of Risk Management System

P	D	C	A
Risk Management Committee and Board of Directors • Develop various measures including the identification of significant risks **Divisions and Group companies** • Formulate annual risk management policies and plans	**Divisions and Group companies** • Establish appropriate rules and work flows • Carry out employee education • Conduct audits and checks	**Divisions and Group companies** • Evaluate the state of implementation and maintenance **Risk Management Committee, CEO and Board of Directors** • Confirm results of evaluation	**Risk Management Committee and Board of Directors** • Discuss various measures of the risk management activity in the next fiscal year

Risk Management System



Under this system, each Canon Inc. division and Group company implements and maintains a self-directed risk management system and makes a yearly report to the Risk Management Committee on the results of its activities.

Having received the report of each subcommittee, division, and Group company, the Risk Management Committee evaluates the state of implementation and maintenance of the risk management system and reports its findings to the CEO and Board of Directors. The evaluation conducted in 2025 found no material flaws in the system.

Group-wide Risk Management Communication

At Canon Inc, during training for newly appointed executives of Group companies, participants are educated on the importance of autonomously implementing and maintaining a risk management system at each company, and the role of executives in implementing and maintaining such a system.

We also distribute the Canon Group Risk Management Handbook to executives and senior managers of Canon Inc. and Group companies in Japan. Moreover, the handbook is used in training for newly appointed general managers and section heads to emphasize the importance of risk management and the role played by managers in building our risk management system.

In addition, an intranet website provides employees of Canon Inc. and Group companies with timely information, including our approach to risk management and updates on activities.

Financial Risk Management

The internal controls for financial reporting used at Canon Inc. are consistent with the basic framework outlined in the On the Revision of the Standards and Practice Standards for Management Assessment and Audit concerning Internal Control Over Financial Reporting (Council Opinions) issued by the Business Accounting Council; these controls are maintained and operated accordingly. The aforementioned Financial Risk Management Subcommittee also conducts activities to strengthen internal controls pertaining to financial risks for the entire Canon Group, including compliance with Japan's Companies Act and Financial Instruments and Exchange Act.

Specifically, we support each Group company to implement independent initiatives and self-driven educational activities, with each company implementing its own PDCA cycle on financial risk-related business procedures to target qualitative improvement in the reliability of the Group's financial reporting.

As a result of these initiatives, we determined that our internal controls over financial reporting as of December 31, 2025 were effective.

Promoting Compliance

The Compliance Subcommittee works to promote corporate ethics across the Group in accordance with the Canon Group Code of Conduct, developing and regularly reviewing the Group's compliance system. As a result of these initiatives, Canon had another year free from material fines or other sanctions in 2025.

Sections of the Canon Group Code of Conduct (Extract)

Management Stance

1. Contribution to Society
- Provision of excellent products • Protection of consumers
- Preservation of the environment
- Social and cultural contributions • Communication

2. Fair Business Activities
- Practice of fair competition
- Observance of corporate ethics
- Appropriate disclosure of information

Code of Conduct for Executives and Employees

1. Compliance with Corporate Ethics and Laws
- Fairness and sincerity • Legal compliance in performance of duties
- Appropriate interpretation of applicable laws, regulations and company rules

2. Management of Corporate Assets and Property
- Strict management of assets and property
- Prohibition against improper use of company assets and property
- Protection of the company's intellectual property rights

3. Management of Information
- Management in compliance with rules
- Prohibition against personal use of confidential and proprietary information
- Prohibition against insider trading
- Prohibition against the unlawful acquisition of confidential or proprietary information pertaining to other companies
- Appropriate use of confidential and proprietary information pertaining to other companies

4. Conflicts of Interests/Separation of Personal and Company Matters
- Avoidance of conflicts of interests
- Prohibition against seeking, accepting or offering improper gifts, entertainment, or other benefits
- Prohibition against acquisition of pre-IPO shares

5. Maintenance and Improvement of Working Environment
- Respect for the individual and prohibition against discrimination
- Prohibition against sexual harassment
- Prohibition against bringing weapons or drugs to the company workplace

Promoting Corporate Ethics

■ Canon Group Code of Conduct and Compliance Card

We have established the Canon Group Code of Conduct to clarify the management stance of the entire Group and the standards that executives and employees must comply with in their duties. To ensure that its content is understood by executives and employees in countries and regions worldwide, in addition to Japanese, the Code of Conduct is translated into more than 20 languages, including English, French, and Chinese, and adopted by a resolution of the Board of Directors of each Group company. A copy of the Code is issued to Group executives and employees worldwide and/or its text is posted on our intranet system as part of further efforts to ensure that it is known and practiced by all.

In addition, a Compliance Card that executives and employees can carry with them has been created in Japanese and more than 20 other languages, including English, French, and Chinese, and issued to Group executives and employees worldwide. Written on one side of the card is the *San-ji* (Three Selfs) Spirit, which has been a guiding principle since our founding, and on the other side is a compliance test that enables employees to conduct a daily self-evaluation.

Compliance Card

■ Corporate Ethics and Compliance Training

Canon carries out corporate ethics and compliance training for executives and employees suited to the circumstances and conditions of the region where they operate.

For example, Canon Inc. and Group companies in Japan conduct relevant training for executives and employees as part of new recruit training, etc. Additionally, we have since 2004 designated a Compliance Week twice a year—once in the first half of the year and the other in the second half—in order to foster discussions in the workplace about compliance issues. Through these efforts, we strive to develop and improve operational processes to ensure that employees are aware of compliance and abide by the law.

■ Compliance Hotline System for Internal and External Whistleblowers

Canon Inc. has a compliance hotline system to handle reports of compliance issues, including violations of laws, bribery and other forms of corruption, and other breaches of the Canon Group Code of Conduct. We encourage appropriate use of the system by using the intranet, compliance training and other means to build awareness.

Canon Inc. also has a hotline for external stakeholders, which they can use to report specific human rights-related concerns and information in connection with Canon's corporate activity or other specific concerns relating to various risks in the supply chain.

With both the internal and external hotlines, due care is taken to protect the privacy of informants and to ensure they do not suffer disadvantageous treatment as a result, including the option of anonymous reporting.

When a report containing a possible compliance violation is received, an investigation is launched to establish the facts and a final decision is made as to whether there is a compliance violation. If a compliance violation is found, the necessary corrective action is taken along with measures to prevent recurrence.

Nearly all Group companies worldwide have a compliance hotline.

Canon Inc. receives biannual reports from Group companies on the operational status of their respective compliance hotline systems. These biannual reports from each Group company include not only the number of cases they received but also a summary of each case, investigation results and responses, and measures to prevent recurrences. Cases at Canon Inc. and Group companies that have been investigated and where compliance violations have been identified are analyzed statistically by category, and the analysis results are reported on a yearly basis to the Risk Management Committee and then fed back to the various Group companies.

The table below shows the numbers of whistleblowing reports, whistleblowing cases and compliance violations recognized after investigation into each case of whistleblowing, over the past three years. There have been no serious compliance violations.

Reports, cases and compliance violations (at year-end)

(no.)

	2023	2024	2025
Reports of whistleblowing during year	298	374	373
Cases of whistleblowing during year	336	409	459
Compliance violations recognized after investigation into whistleblowing	43	66	62

* In cases where a single report contains multiple complaints, it is treated as one report and each complaint is counted as a separate case.

Compliance System

We have identified the significant compliance violation risks that Canon may face in the course of business (for example, violations of competition laws, anti-bribery laws and export control regulations) based on an assessment of the likelihood of the risk materializing and the scale of its potential impact on our business. To reduce these risks, we are working to improve the system to ensure legal compliance by improving operational workflows and rules, providing compliance training to applicable employees, and conducting audits and checks.

■ Strict Compliance with Security Trade Control

Canon implements a security trade control framework headed by the President. The framework ensures that we comply with regulations on the export of goods and technologies that could be diverted for use in weapons of mass destruction or conventional weaponry. Specifically, prior to entering into business we strictly check such issues as whether export goods and technologies are controlled by regulations, or whether counterparties are engaged in the development of weapons of mass destruction.

Security Trade Control is insufficient if undertaken by a single country or region. It is important to have international cooperation based on international treaties and export control regime agreements. To provide a unified policy and standard in the field of Security Trade Control, we established the Canon Security Trade Control Guidelines, which is implemented at Group companies worldwide.

In recent years there has been a move to use regulatory frameworks for security trade control in order to restrict the transactions of certain countries, regions, or corporations, mainly for reasons related to competition in the development of advanced technologies, information security, and protection of human rights. As it expands its range of business fields, Canon has also seen an increase in business transactions that require careful attention. We will pay close attention to the international situation and to the latest regulatory trends in our activities to ensure full compliance with Security Trade Control.

■ Compliance with Competition Laws

Business divisions of Canon Inc. and Group companies worldwide with sales and service functions conduct regular training for employees of divisions exposed to the risk of competition law violations to educate them about competition laws, give examples of legal violations, and provide everyday operational compliance guidance. Employees are encouraged to make use of Canon's competition law hotline (connected to the Legal Division) when unsure of how to interpret or apply competition laws.

■ Prevention of Corruption

The Canon Group Code of Conduct (→P88) clearly stipulates that Group executives and employees are prohibited from receiving benefits from business partners and corporate customers in the form of gifts or entertainment, etc., that exceed the social norm, and from providing similar benefits to government agencies, business partners, and corporate customers. It also clearly prohibits actions that may cause conflicts of interest or constitute insider trading. For our suppliers, we have formulated the Canon Supplier Code of Conduct, which requires them to refrain from engaging in any form of corruption, including bribery.

Based on the above policy, following identification and assessment of the risks that Canon may face in conducting business, the Risk Management Committee has identified violation of anti-corruption laws as a significant risk. As a countermeasure, corruption risk is assessed based on the country/region and type of business using such references as the Corruption Perceptions Index published by Transparency International, and then depending on such risk, anticorruption systems are established in accordance with laws and guidelines related to anti-corruption in major countries, such as the Foreign Corrupt Practices Act (FCPA) of the United States and the Bribery Act of the United Kingdom. Specifically, for businesses and regions assessed as high risk, each Group company has established a responsible division and has clarified its management stance on anti-corruption and matters to be observed through the formulation of basic policies and company rules on anti-corruption. We are also putting in place systems to prevent corruption among suppliers, intermediaries, and other third parties outside Canon (performance of due diligence and inclusion of an anti-bribery clause in the contract) and conduct annual training for employees engaged in high-risk duties to deepen their understanding of the anticorruption laws and regulations in major countries and regions. Moreover, we not only conduct audits depending on the risk of corruption but also conduct an annual survey (→P77) of suppliers as part of our supply chain management to check whether measures are in place to prevent the acceptance of bribes or inappropriate benefits. Finally, the Risk Management Committee undertakes an annual evaluation of the implementation and maintenance of the risk management system, which includes such anticorruption systems, and reports the results of such evaluations to the CEO and Board of Directors.

Reference: Canon Suppliers Code of Conduct
https://global.canon/en/procurement/pdf/coc-e.pdf

■ Protecting Personal Information

Based on its Personal Information Protection Policy, Canon Inc. has drawn up and is improving its internal rules for processing of personal information, including its Personal Information Protection Regulation.

The Risk Management Committee has also identified violation of the Protection of Personal Information Act as a significant legal risk for Canon. Accordingly, besides keeping abreast of related regulatory trends, Group companies worldwide are working to build systems where all personal information is properly acquired, utilized and managed, through the application of internal controls, regular self-audits, and education programs.

Major privacy legislation affecting Canon

Japan	Act on the Protection of Personal Information
EU	General Data Protection Regulation (GDPR)
The State of California, U.S.	California Consumer Privacy Act
China	Personal Information Protection Law

Promoting Business Risk Management

The Business Risk Management Subcommittee is responsible for identifying significant operational risks in terms of their potential impact and managing them.

Action policies and plans for each identified significant risk are decided in cooperation with the responsible divisions across the Group, and system implementation and risk mitigation activities are promoted through each business division and the responsible division at each Group company.

Business Continuity Plan

Canon's Headquarters building and core facilities for information systems and research and development are concentrated in suburban areas of Tokyo. As the incidence of earthquakes in Japan is relatively high, it is also at greater risk of earthquake damage than other countries and regions. Canon also has a global network of facilities and offices. The occurrence of earthquakes, floods, other natural disasters, or terrorist attacks could cause disruption of the infrastructure for such facilities and offices. Canon believes that establishing a system to ensure that business operations can continue in the event of such a natural disaster or emergency represents one of the most important social responsibilities of any company. Based on this recognition, we have formulated a business continuity plan (BCP)*1 and Canon Group Disaster Preparedness Guidelines, and are taking other measures to ensure business continuity in the event of a disaster. Such measures include putting in place a backup system based on parallel production of similar models at a number of sites, upgrading buildings constructed according to old aseismic design standards, concluding disaster agreements with local communities, and developing systems for collecting information and reporting.

Due to the critical importance of our Shimomaruko headquarters in Tokyo, Japan, as the home base for all Group operations, we have established a crisis control center, installed backup generators, stockpiled fuel, equipment, and supplies, and established a multiplex communication system. Moreover, we set up a Disaster Recovery Center*2 to back up information systems to ensure that the core IT system will operate securely in the event of a large-scale disaster such as an inland earthquake in the Tokyo capital region.

We have updated all Group company facilities in Japan, setting up emergency communications equipment and support structures, and inculcated a sense of readiness in our employees through practical disaster-preparedness training. We also have systems that use data from surveillance cameras installed at each Group site so that any damage caused by natural disasters or other emergencies can be evaluated swiftly. Furthermore, we have prepared a leader's manual in order to safeguard human life immediately following a natural disaster or fire, prevent secondary disasters, and protect company assets. Using this manual as a model, Group companies are also creating localized manuals based on the unique risks in the areas where they operate to facilitate the smooth restoration of services in the event of a disaster. Last year, 45 operational sites conducted emergency drills based on these manuals.

*1 An action plan that includes measures to provide for the continuation of a minimal level of business in the event of disaster, accident, or other such event, and to restore operations promptly.
*2 A facility prepared for data backup in the event of a system breakdown due to a disaster.

Economic Security Initiatives

In response to the recent rise in geopolitical risk, activities to promote economic security by maintaining and reinforcing factors such as strategic autonomy and strategic indispensability – the stated aims of Japan's Economic Security Promotion Act, enacted in May 2022 – have gained in importance. This includes stronger initiatives to prevent technology outflows and the introduction of new export controls with expanded scope.

In addressing economic security issues, Canon Inc. collates, researches, and analyzes related internal and external information, sharing and reporting appropriately with management and the relevant divisions to promote the Group's economic security activities while bolstering related risk mitigation capabilities.

Proper Payment of Taxes

Canon believes that, as a multinational corporation with operations spanning the globe, the proper payment of taxes in the countries and regions where it operates is one of its most fundamental and important social responsibilities. Accordingly, Canon Inc.'s Finance & Accounting Headquarters operates an integrated tax management system in accordance with the principles set out below. As a result, Canon did not receive any negative tax-related judgments or assessments in 2025, nor was it subject to any major punitive measures, such as fines.

1. Pay taxes properly in accordance with the letter and the spirit of tax-related laws and ordinances without employing tax planning for tax avoidance purposes.
2. Ensure that tax accounting and other related processes are carried out unfailingly, according to law.
3. Develop tax-related governance systems and work to raise awareness about tax compliance.
4. Adhere to common international rules on international taxation (guidelines set by the Organization for Economic Co-operation and Development and the United Nations) and ensure that actions are in compliance with the tax laws of each country.

Corporate Income Taxes

	2021	2022	2023	2024	2025
Taxes on income before income taxes (hundred million yen)	719	924	1,063	1,183	1,239
Effective tax rate on income before income taxes (%)	23.7	26.2	27.2	39.3	25.7

Addressing Risks in the Development and Use of AI Technology

Canon is striving to hone the competitiveness of its products by incorporating proprietary AI technology into products and services in various business domains. We have a track-record of capitalizing on AI technology to launch products with significantly enhanced performance and functionality, primarily in the Imaging and Medical businesses, but are further incorporating AI technology into our products and extending this technology to all business groups, including the Printing and Industrial businesses. Additionally, by developing and providing AI technology-based services in the various businesses, we are helping to transform the business processes of our customers. Canon is also actively leveraging generative AI in in-house operations to pursue operational reforms and boost productivity.

Meanwhile, developing and harnessing rapidly evolving AI technology for Canon's products and services requires compliance with AI-related laws and regulations being formulated in various countries and regions. Even in cases where AI does not fall under regulations, consideration must be given to the ethical aspects of this technology, including biased judgments, the output of erroneous information, and unexpected behavior. Moreover, with regard to the use of generative AI, there is a need to prevent risks such as copyright and trademark infringement, breaches of confidential information, and unauthorized access.

Addressing AI Risks

Canon Inc. has established a Group-wide framework for assessing and responding to AI risks to ensure that we provide safe and secure AI products and services while complying with legal and ethical requirements for AI. To address all such risks, including risks related to ethical considerations, in addition to the legal and regulatory requirements of various countries and regions, we have prepared our own AI risk assessment checklist, which includes evaluation criteria such as fairness, transparency, appropriate use, safety and robustness, and privacy and security. We use this checklist to assess AI risks at appropriate stages of the product development process (e.g., in planning and at completion), and obtain final approval after taking any needed steps, thus seeking to minimize AI risks in our products and services. We have also established a dedicated organization to address AI risks, which works with the Quality Assurance and Legal divisions to deploy measures across the Canon Group.

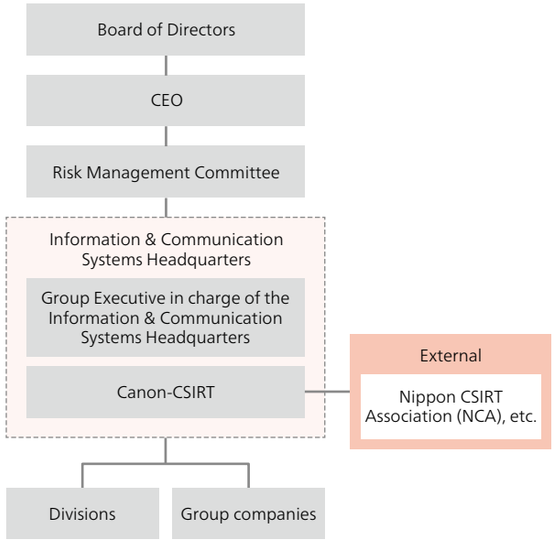
Regarding generative AI, we have established a company-wide cross-functional organization to develop rules for use and educational programs. We are working to improve awareness and literacy regarding intellectual property rights and information security through training for all employees. Furthermore, we are working to mitigate risks to the infrastructure by selecting and rolling out AI services that incorporate advanced security. Through these steps, we are working to boost work productivity while ensuring safety in the use of generative AI.

Information Security

Basic Approach

Recognizing it as a vital management issue, Canon conducts Group-wide information security initiatives in line with the fundamental principles of information security regulations. Since information security poses potentially major and direct business risks to Canon operations, we have created an information security promotion system as part of our risk management approach (→P87).

Information Security Promotion System



Information Security Promotion System

Canon has constructed a system for the rapid collection and reporting of information on any information security-related incidents, based on the Risk Management Committee (→P87) established through a Board resolution.

Any incidents that occur must be reported to the Information & Communication Systems Headquarters. Depending on the circumstances and the business implications, they are also reported to the CEO and Board of Directors via the Risk Management Committee. Canon has also designated the senior executive in charge of information security at Canon Inc. as the Group Executive in charge of the Information & Communication Systems Headquarters. The executive has decision-making responsibility for information security measures and is tasked with managing information security across the entire Group.

The Information & Communication Systems Headquarters is also responsible for any input into medium-term business planning relating to information security, prior to CEO approval.

CSIRT* is a dedicated team for dealing with information security incidents established inside the Information & Communication Systems Headquarters. Canon CSIRT joined the Nippon CSIRT Association (NCA) to strengthen collaboration with CISRTs of other companies.

The Information & Communication Systems Headquarters formulated the Canon Group Information Security Rules to ensure that uniform measures and a consistent approach to information security are applied across the Group, both in Japan and overseas.

Each Group company creates regulations and guidelines based on these rules in line with its needs and conducts related training and awareness activities.

* Computer Security Incident Response Team. This is a dedicated, organized group that deals with incidents involving computer security.

Information Security Management System

Information Security Training & Development

In order to maintain and improve information security, Canon is focusing on raising awareness among employees who use information systems.

Canon executives and all employees undergo annual information security training using an online platform. Roughly 23,000 employees of Canon Inc. received the information security training in 2025. Course content focused on improving information security literacy, including ways of identifying suspicious emails, vulnerability risks and related mitigation measures, and critical points to consider when web conferencing.

In addition, special training sessions based on a targeted email attack were conducted involving roughly 60,000 Canon Inc. and Group company employees. This was intended to provide practical instruction in how to respond appropriately to suspicious emails and thus avert widespread damage. Specifically, newly hired employees unaccustomed to using email in the work environment received separate training to reinforce their awareness.

Information Security Audits

The status of each Group company's information security measures is confirmed by means of internal inspections based on the "Canon Group Information Security Policy" as well as through periodic audits by the Information and Communications Systems Headquarters, and improvements or revisions are made as needed.

In 2025, information security audits were conducted at 23 Group companies in Japan and 28 Group companies overseas. No major security risks with business implications were detected through these audits.

External Certification

Canon Inc.'s information security division has acquired ISO 27001 certification, the international standard for building and operating information security management systems.

Information Security Initiatives

Information System Security Measures

As part of measures to prevent the leakage of confidential data, we ensure that critical information is stored using a dedicated, access-controlled system with reinforced security and auto-recorded user activity. In addition, we have established an environment in which employees can safely access the company's information assets from outside the office, and we also carefully manage email attachments as well as the taking of company computers and storage media offsite.

As a measure against cyber-attacks, we use monitoring systems to identify any suspicious emails with possible malware attachments. We also monitor unauthorized online communications to try and prevent attacks from causing more widespread damage.

In addition, we have participated each year since 2017 in cyber-attack response training (NISC*/NCA affiliated cross-field company-wide training), in order to strengthen our system for countering obstructions.

* National center of Incident readiness and Strategy for Cybersecurity.

Security Measures for Production Facilities

Canon implements security measures for its production facilities to ensure malware, cyberattacks or other information security issues do not reduce productive capacity or otherwise disrupt production plans.

In the past, corporate mainframes or online information systems were the major targets for cyberattacks. Today, the growing use of off-the-shelf OS software and IoT means that production facilities attract the same level of information security risk. A separate approach is needed for production systems because production lead-times are longer than the customer support periods for off-the-shelf OS software. To ensure that Canon Inc. and Group manufacturing companies in Japan and overseas do not have to suspend operations due to a virus infection or similar attack, we also monitor the networks linked to important facilities and production lines for any unauthorized activity.

We also conduct security audits of production facilities to maintain a safe production environment.

Product/Service Security Measures

Canon is engaged in initiatives to prevent any cybersecurity risks with products or services before they appear. In addition, our systems are designed to try to minimize the customer impacts if a cyber-security incident occurred.

See Product/Service Security Measures (→P74).

Security Measures for Supply Chain

Risks have grown in recent years of an attack against one part of the supply chain impacting the entire chain, leading to interruptions in the supply of products and services or the leaking of confidential information. In turn, this could result in economic damage, the loss of credibility and brand value, or other negative outcomes.

To mitigate such risks, Canon Inc. is engaging with suppliers through information sharing and other cooperative efforts aimed at reducing information security risks within the entire supply chain.