Risk Management

Canon's Approach

Canon Inc. recognizes that to ensure the proper operation of the Canon Group and to continually improve corporate value, implementation and maintenance of a risk management system to deal with serious 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 executive vice president, the committee has established three subcommittees: the Financial Risk Management Subcommittee, Compliance Subcommittee, and Business Risk Management Subcommittee.
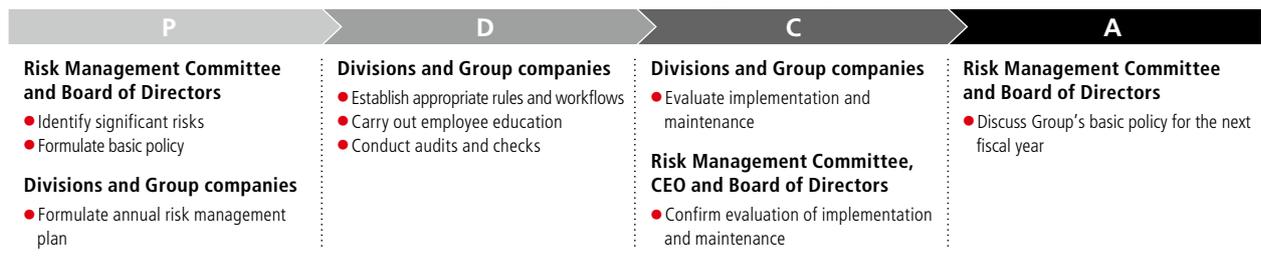
The Risk Management Committee develops various measures to promote the Group's risk management activities, including identifying any significant risks (violations of laws and regulations, inappropriate financial reporting, quality issues or information leaks, etc.) that the Group may face in the course of business.
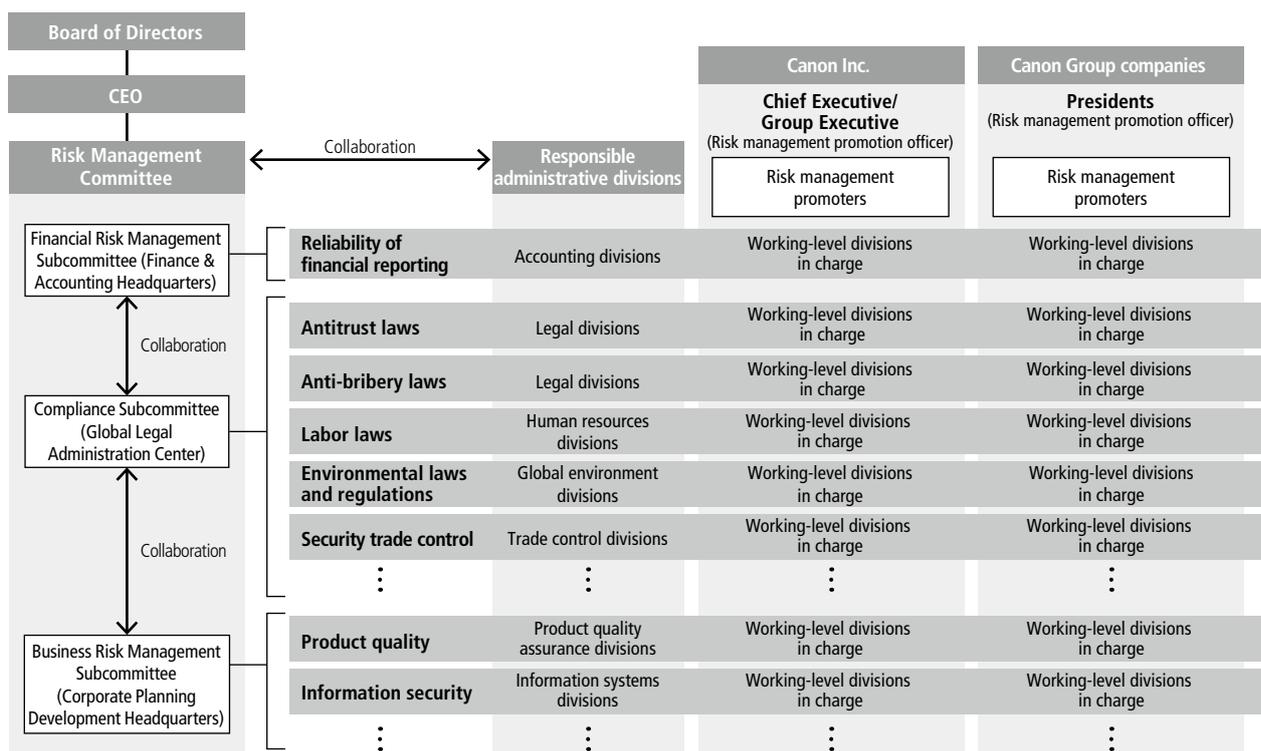
The Committee also creates an annual basic policy for risk management activities and, after obtaining the approval of the Board of Directors, carries out risk management activities within Canon Inc. divisions and Group companies. The Committee evaluates the improvement and implementation of the risk management system for each division and Group company, and reports the results of such evaluations to the CEO and Board of Directors. Results of evaluations conducted in 2019 showed no material flaws in the system.

In line with the basic policy prepared by the Committee and in their capacity as risk management promotion officer, the heads of Canon Inc. divisions and presidents of Group companies each formulate an annual risk management plan for their own division or Group company, and assume responsibility for

Processes for Implementation and Maintenance of Risk Management System

P	D	C	A
Risk Management Committee and Board of Directors ● Identify significant risks ● Formulate basic policy **Divisions and Group companies** ● Formulate annual risk management plan	**Divisions and Group companies** ● Establish appropriate rules and workflows ● Carry out employee education ● Conduct audits and checks	**Divisions and Group companies** ● Evaluate implementation and maintenance **Risk Management Committee, CEO and Board of Directors** ● Confirm evaluation of implementation and maintenance	**Risk Management Committee and Board of Directors** ● Discuss Group's basic policy for the next fiscal year

Risk Management Promotion System

promoting related risk management activities. Risk management promoters appointed within each division and Group company assist risk management promotion officers in coordinating risk management practices.

Additionally, Canon Inc. administrative divisions responsible for various risks associated with business activities, including the Legal Division, Human Resources Division, Security Trade Control Division, and Quality Assurance Division, control and support the risk management activities of each division and Group company.

Group-wide Risk Management Communication

During training for newly appointed Group executives conducted by the Human Resources Division at Canon Inc., 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.

Furthermore, at Canon Inc. and Group companies in Japan, we distribute the Canon Group Risk Management Handbook to directors and executives. The handbook explains the significance of risk management, the Group's risk management system, our approach to implementing risk management and the role of management. When the Human Resources Division conducts training for newly appointed general managers and managers, it uses the handbook to educate them on the importance of risk management and the role of management in constructing the risk management system.

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

Financial Risk Management

The Financial Risk Management Subcommittee carries out 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 as well as the United States' Sarbanes-Oxley Act.

We endeavor to make qualitative improvements in ensuring the reliability of the Group's financial reporting. We support independent initiatives and self-driven educational activities at Group companies as they implement the PDCA cycle (review business procedures for financial risk).

As a result of these initiatives, Canon's accounting auditor determined that the company's internal controls related to financial reporting were effective in fiscal 2019.

Promoting Compliance

The Compliance Subcommittee works to promote corporate ethics across the Group in accordance with the Canon Group Code of Conduct, and to improve the Group's legal risk management system. As a result of these initiatives, Canon had another year free from material fines or other sanctions in 2019.

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
Canon established the Canon Code of Conduct in 1992, and later updated it as the Canon Group Code of Conduct in 2001. It clarifies the Group's management stance and standards that Group executives and employees must comply with in their duties. In addition to Japanese, the Code of Conduct has been 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, which also strives to ensure that it is known and practiced by all.

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

CANON "San-Ji" Spirit

Ji-hatsu (Self-Motivation)
Take the initiative and be proactive in everything you do

Ji-chi (Self-Management)
Conduct yourself responsibly and be accountable for all of your actions

Ji-kaku (Self-Awareness)
Understand the situation you find yourself in and your role in that situation

Our commitment under the "San-Ji" Spirit:
- We must observe and act in accordance with all applicable laws and rules.
- We must always conduct ourselves in a fair, honest and ethical manner.

Canon

Compliance Test

Would your actions

☐ violate any laws or rules?
☐ leave you feeling guilty?
☐ disappoint your family, friends or co-workers?
☐ embarrass you if reported publicly in the news?
☐ cause trouble for the community?
☐ harm the Canon Brand?

When in doubt, always consult your superior or the designated department.

Compliance Card

■ Corporate Ethics and Compliance Training
Canon carries out corporate ethics and compliance training for employees suited to the circumstances and conditions of the region where they operate.

For example, Canon Inc. conducts relevant training as part of rank-based training for newly appointed general managers and managers as well as new employees.

Additionally, Canon Inc. and its subsidiaries in Japan 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
Canon Inc. has established a Compliance Hotline system to receive information related to compliance issues. The confidentiality of reporters is strictly maintained, and they are guaranteed not to suffer any unfair treatment for using the system. We continually work to encourage appropriate use of the system by expounding the purpose of the system through such means as the intranet compliance website and compliance training, etc.

The system also has been established at nearly all Group companies worldwide. Canon Inc. receives biannual reports from Group companies on the operational status of their respective Compliance Hotline systems. Over the past few years, the total number of cases filed using the system at Group companies overall has been around 300-400 per year.

These biannual reports from each company include not only the number of cases filed, but also a summary of each case, the results of investigation and response, and measures to prevent recurrences. Each Group company takes the necessary corrective measures and recurrence prevention measures based on the investigation results.

Legal Risk Management System
At Canon, we have identified significant legal risks that the Group may face in the course of business operations (for example, violations of antitrust laws, anti-bribery laws and export control regulations) by considering the likelihood and impacts on Canon's business. To minimize 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 Export Control Regulations
Canon Inc. 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, 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. Furthermore, in the field of security trade controls, we have also established and implemented the Canon Security Trade Control Guidelines to provide a unified control policy and standard for the Group. At the same time, we hold regular briefings, training sessions and e-learning courses for persons responsible for security trade controls at Canon Inc. and Group companies worldwide.

Security trade controls are insufficient if undertaken by a single country. It is important to have international cooperation based on UN and international export control regime agreements. Recently, there has been a growing movement of using trade control regulations to restrict the transactions of particular countries or corporations. Canon has also seen an increase in business transactions that require careful attention as it acquires various new businesses. We will pay close attention to the latest trends in trade controls in our activities.

■ Compliance with Antitrust Laws
Canon recognizes that compliance with antitrust laws, which apply to all of its business activities, from product development to production, sales and after-sales service, is absolutely vital.

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 antitrust violations to educate them about antitrust laws, give examples of legal violations, and provide everyday operational compliance guidance. Employees are encouraged to make use of Canon's antitrust law hotline (connected to the Legal Division) when unsure of how to interpret or apply antitrust laws.

■ Prevention of Bribery
The Canon Group Code of Conduct (→P103) 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, or provide similar benefits to government agencies, business partners and corporate customers. In addition, the Canon Group CSR Basic Statement (→P111) includes "9. Prevent corruption in all its forms including bribery," making clear to all stakeholders Canon's management stance.

Under the above policy, Canon's Risk Management Committee has identified the risk of violations of anti-bribery laws as a significant risk. The Committee has established a bribery prevention system in accordance with the risk for each Group company calculated based on the countries and regions where it does business and its business activities. In doing so, we have followed laws and guidelines on bribery prevention in major countries, such as the U.S. Foreign Corrupt Practices Act and the U.K. Bribery Act. Specifically, a responsible division has been established at each Group company, and our management stance on bribery prevention has been clarified along with points to be observed through the formulation of a basic policy on bribery prevention and company rules. Moreover, we conduct due diligence on business partners and include anti-bribery clauses in our contracts with them. We also conduct annual training for employees engaged in high-risk duties to deepen their understanding of anti-bribery laws in major countries and Canon's Code of Conduct.

In addition, in response to the above-mentioned Basic Statement, we have issued to suppliers the Canon Supplier CSR Guidelines (→P114), which requires Canon suppliers to prevent corruption in all its forms, including bribery. Moreover, in our annual surveys (→P115) conducted to suppliers as part of our supply chain management, we check whether measures are in place to prevent the acceptance of bribes or inappropriate benefits.

■ Protecting Personal Information
Canon strives to ensure proper handling of personal information (including personally identifiable information, or PII).

At Canon Inc., we have created rules to safeguard personal information, including a Personal Information Protection Policy and Personal Information Protection Rules, and conduct training and audits regularly as part of our system to prevent leaks of information.

Starting in 2015, we expanded the scope of these activities to include all Group companies, creating a centralized management system covering the entire Group. As a result, in 2019 the Group had another year free of serious incidents involving the loss or leakage of personal information, and did not receive any privacy infringement complaints from customers.

Canon Inc. and Group companies in Japan have also implemented measures to deal with Japan's Social Security and Tax Number System (referred to as the "My Number" system), introduced in 2016, in an appropriate manner. All Group companies in Japan formulated My Number Handling Rules, My Number Regulations, and a detailed handling procedure manual. In particular, our measures regarding physical and technological security are more stringent than those mandated by law, and we continue to collaborate with the IT Division on this matter. Moreover, in regard to the EU's General Data Protection Regulation (GDPR), implemented in May 2018, Canon Inc. entrenched the systems and compliance rules that it established in 2018.

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

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

Ensuring Complete Information Security
Recognizing that information security is a vital management task, Canon has established an appropriate management system for the entire Group, in accordance with the fundamental principles of information security regulations. The steps that we take under this system include measures to prevent leaks of confidential information, handle external cyber-attacks, bolster information security at production facilities, and provide information security training to raise employee awareness.

Moreover, Canon has maintained ISO27001 certification for its information security management systems since 2005.

■ **Information Security Management System Operations**
The Group Executive in charge of the Information & Communication Systems Headquarters is the senior executive in charge of information security at Canon Inc. and has decision-making responsibility for information security measures. The executive oversees the Information & Communication Systems Headquarters, which is the organization responsible for managing information security across the Canon Group.

If an information security incident occurs, the matter must be reported to the Information & Communication Systems Headquarters. It may also be reported to the Risk Management Committee (→P102), depending on circumstances.

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 globally. Each Group company creates regulations and guidelines based on these rules in line with its needs, and conducts related training and awareness activities. Periodic inspections are also carried out to assess the status of each Group company's information security measures and enable improvements or revisions as needed.

In 2019, information security checks were again carried out at 24 Group companies in Japan and 24 Group companies overseas.

CSIRT*, a dedicated team for dealing with information security incidents, was created within Canon Inc.'s Information & Communication Systems Headquarters in 2015. At that time, Canon joined the Nippon CSIRT Association (NCA) to strengthen collaboration with CSIRTs in other companies.

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

■ **Information System Security Measures**
Canon implements measures to safeguard the three elements of information security: confidentiality, integrity, and availability[1].

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 while away on a business trip, and we have also placed restrictions on email attachments and taking company computers and storage media offsite.

As a measure against cyber-attacks, we use monitoring systems to identify any suspicious emails with possible malware[2] attachments. We also monitor unauthorized online communications from internal sources to try and prevent attacks from causing more widespread damage.

In addition, we have strengthened countermeasures in anticipation of cyber-attacks on our global sites in conjunction with the Olympic and Paralympic Games Tokyo 2020. We have also participated each year since 2017 in cyber-attack response training (NISC[3]/NCA affiliated cross-field companywide training), in order to strengthen our system for countering obstructions.

[1] Confidentiality: Enable only authorized personnel to access information.
Integrity: Ensure data and processing methods are accurate and cannot be modified without authorization.
Availability: Make data accessible to authorized personnel when needed.
[2] Malware: malicious software (including computer viruses and ransomware) created with the deliberate intention of performing unauthorized or harmful operations.
[3] NISC: 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, cyber-attacks 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 cyber-attacks. 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 production companies worldwide 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.

■ **Information Security Training to Raise Employee Awareness**
In order to maintain and improve information security, Canon is focusing on raising awareness among employees who use information systems.

Both regular and mid-career hires are thoroughly trained on Canon's information security measures and rules through group training. In addition, all employees undergo annual information security training using our e-learning system.

In 2019, roughly 25,000 employees—equivalent to Canon Inc.'s total workforce—received information

security training. This included training to develop information security literacy*, including how to deal with suspicious emails, measures to prevent email misdirection, and other IT protocols. In addition, special training sessions based on a targeted email attack were conducted involving roughly 78,000 Canon Inc. and Group company employees to provide practical instruction in responding appropriately to suspicious emails so widespread damage is avoided.

* Information security literacy: knowledge and skills needed to implement proper information security measures.

Post-Disaster Business Continuity Plan

■ Responding to the Risk of Damage to Infrastructure

Canon believes that establishing a system to ensure that business operations can continue after 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 working hard on advancing business continuity measures for disasters, including 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 rebuilt all on-site buildings, 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 disaster.

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 Canon 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, 40 operational sites conducted emergency drills based on these manuals.

*1 Business Continuity Plan (BCP): 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 Disaster Recovery Center: a facility prepared for data backup in the event of a system breakdown due to a disaster.

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 abides by the following principles on tax matters. In 2019, Canon did not receive any negative tax-related judgments or assessments, nor was it subject to any major punitive measures, such as fines.

1. Pay taxes properly in accordance with tax-related laws and ordinances.
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

	2015	2016	2017	2018	2019
Taxes on income before income taxes (hundred million yen)	1,161	827	980	962	562
Effective tax rate on income before income taxes (%)	33.4	33.8	27.7	26.5	28.7

Measures to Prevent Infection with Novel Coronavirus

We have established a team to take countermeasures against infection with the novel coronavirus (COVID-19) that was declared a pandemic by the World Health Organization (WHO) in March 2020. To ensure the safety of all Group employees, we are calling on everyone to take thorough measures to prevent infection, as well as cancelling large events in and outside the company, staggering working hours, and implementing remote working in an effort to prevent the spread of infection. We are also working to shut the virus down as quickly as possible by developing a genetic testing system for novel coronavirus and providing x-ray and CT diagnostic equipments.