

# Risk Management

## Basic 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

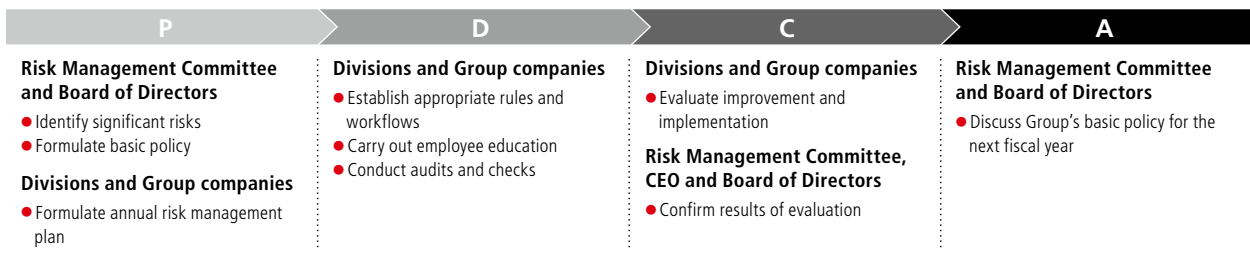
Canon Inc. has established a risk management committee based on a resolution of the Board of Directors. Chaired by the Executive Vice President, the committee has established three subcommittees: the Financial Risk Management Subcommittee, Compliance Subcommittee, and Business Risk Management Subcommittee.

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, environmental issues, 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 2020 showed no material flaws in the system.

## Processes for Implementation and Maintenance of Risk Management System



In line with the basic policy prepared by the Risk Management Committee and in their capacity as risk management promotion officers, 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 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

Canon Inc.'s internal control over financial reporting is maintained and performed in accordance with the criteria established in Internal Control – Integrated Framework (2013) issued by the Committee of

Sponsoring Organizations of the Treadway Commission (“COSO”). 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 to review business procedures for financial risk.

### 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 2020.

### 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. To ensure that its content is understood by executives and employees in countries and regions worldwide, 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. A copy of the Code is issued to all executives and employees and its text is posted on the intranet system as part of further efforts to ensure that it is known and practiced by all.

In addition, a Compliance Card that employees can carry around 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 Selves) 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.



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. and Group companies in Japan conduct relevant training for executives and employees as part of new recruit training. 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 established a compliance hotline system to receive information related to compliance issues, including violations of laws or Canon Group Code of Conduct regulations. The confidentiality of informants is strictly maintained, and protection against workplace retaliation is guaranteed. We continually work to encourage appropriate use of the system by promoting awareness of it through such means as the intranet compliance website and compliance training. When a report is received of a possible compliance violation, an investigation is launched to establish the facts and a final decision is made as to whether infringement has taken place. If a compliance violation is determined to have occurred, the necessary corrective action is taken along with measures to prevent recurrence.

An internal reporting system has also 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. 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.

Canon has also set up hotlines for external stakeholders which they can use to report specific concerns in the Canon supply chain, for instance human rights issues such as child labor and forced labor or occupational health and safety issues. When a report is received, an investigation is launched to establish the facts and, where necessary, corrective action is taken along with measures to prevent recurrence.

The number of reports received in 2020 by the entire Group with its 181,897 employees was 302, mainly from Asia (including Japan) and the Americas. Of those with investigation completed as of the end of 2020, compliance violations were confirmed in 52 cases. The reports received in 2020 included no serious compliance violations.

**Compliance System**

We have identified the significant compliance violation risks that the Canon Group may face in the course of business (for example, violations of antitrust 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 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 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 before entering into business 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 controls are insufficient if undertaken by a single country or region. It is important to have international cooperation based on UN and international export control regime agreements. To provide a unified Group-wide policy and standard in the field of security trade controls, the Canon Group has established the Canon Security Trade Control Guidelines, which are implemented at Canon Inc. and Group companies worldwide.

Recent years have seen a movement toward the use of security trade control regulations to restrict the transactions of particular countries, regions, or corporations for reasons related mainly 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 controls.

■ 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 Corruption

The Canon Group CSR Basic Statement (→P41) includes "9. Prevent corruption in all its forms including bribery," making clear to all stakeholders, both internal and external, the management stance adopted by

Canon on bribery and other forms of corruption. In addition, the Canon Group Code of Conduct (→P105) 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 and insider dealing. In line with the above Basic Statement, we have formulated the Canon Supplier Code of Conduct, which requires our suppliers to refrain from engaging in any form of corruption, including bribery.

Based on the above policy, following identification and assessment of the risks that the Canon Group may face in the course of business, the Risk Management Committee has identified violation of anti-bribery laws as a significant risk. As a countermeasure, the risk of corruption is assessed based on the country/region and type of business using the Corruption Perceptions Index published by Transparency International, and depending on such risk, anti-corruption 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 external to the Canon Group (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 anti-corruption laws and regulations in major countries and regions. Moreover, we not only conduct audits depending on the risk of corruption but also conduct annual survey (→P92) 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 improvement and implementation of the risk management system, which includes such anti-corruption system, and reports the results of such evaluations to the CEO and Board of Directors.

In 2020, Canon was not subject to any fines, penalties, or other sanctions in connection with violations of anti-corruption laws or regulations.

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

#### ■ 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 Group companies, creating a centralized management system covering the entire Group. As a result, in 2020 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.

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. The year 2020 saw active moves worldwide to strengthen the regulatory protection of personal information, exemplified by the amendment of Japan's Act on the Protection of Personal Information, the enactment of the California Consumer Privacy Act in the United States, and the opening to public comment of China's draft Personal Information Protection Law. Canon is monitoring these legislative trends and will respond appropriately.

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

■ **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 (→P104), 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. The status of each Group company's information security measures is confirmed by means of the companies' internal inspections based on a common set of rules as well as through periodic audits by the Information and Communications Systems Headquarters, and improvements or revisions are made as needed.

In 2020, information security checks were again carried out at 23 Group companies in Japan and 26 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.

\* 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 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\*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 participated each year since 2017 in cyber-attack response training (NISC\*3/NCA affiliated cross-field company-wide 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 Malicious software (including computer viruses and ransomware) created with the deliberate intention of performing unauthorized or harmful operations.

\*3 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 manufacturing 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 2020, roughly 25,000 employees—equivalent to Canon Inc.'s total workforce—received information security training. Participants studied examples of information security incidents, heightened their alertness to the risk of computer viruses, and learned precautions to take when using information infrastructure as part of a curriculum designed to improve information security literacy.\* In addition, special training sessions based on a targeted email attack were conducted involving roughly 93,000 Canon Inc. and Group company employees to provide practical

instruction in responding appropriately to suspicious emails and thus averting widespread damage.

\* Knowledge and skills needed to implement proper information security measures.

### 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 engaged in research and development, procurement, production, logistics, marketing, and servicing. 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)\*<sup>1</sup> 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 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\*<sup>2</sup> 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, 43 operational sites conducted emergency drills based on these manuals.

The global COVID-19 pandemic had an initial disruptive effect on our supply chains and production sites around the world, to which we responded with measures including temporary suspension of operations or reduction of output at certain plants. Since then, the state of emergency declared by the Japanese government, together with lockdowns in countries around the world, curfews, and other restrictions have had a limiting effect on economic activity, and the associated closure of offices and retail stores, limiting of international travel, and restricted availability of international cargo shipment have contributed to a corresponding negative effect on the sales activity. Our response to these circumstances has included establishing a response team, cancelling large events in and outside the company, staggering working hours, and implementing remote working in an effort to prevent the spread of infection. At the same time, by adapting to the changed external environment, we are working to restore production and sales activities globally.

\*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.

### 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 2020, 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 unflinchingly, 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

	2016	2017	2018	2019	2020
Taxes on income before income taxes (hundred million yen)	827	980	962	562	343
Effective tax rate on income before income taxes (%)	33.8	27.7	26.5	28.7	26.4