Risk Management

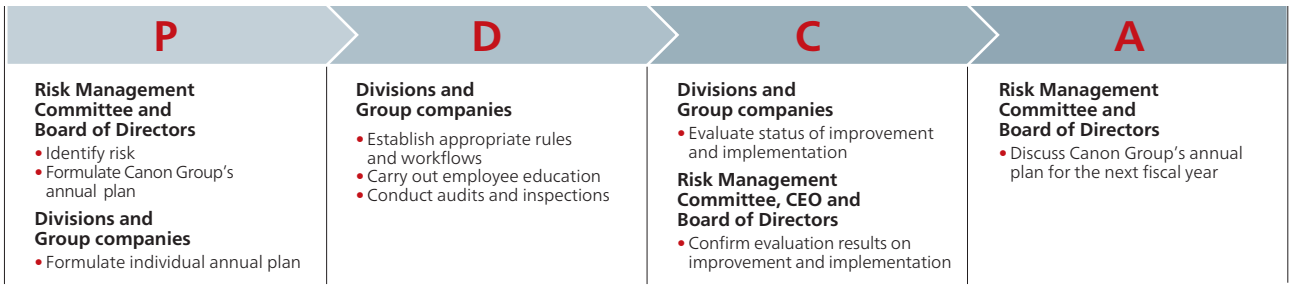
Risk Management System

Canon Inc. has established the Risk Management Committee based on a resolution passed by its Board of Directors. This committee is comprised of three subcommittees, namely, the Financial Risk Management Subcommittee, Compliance Subcommittee, and Business Risk Management Subcommittee.

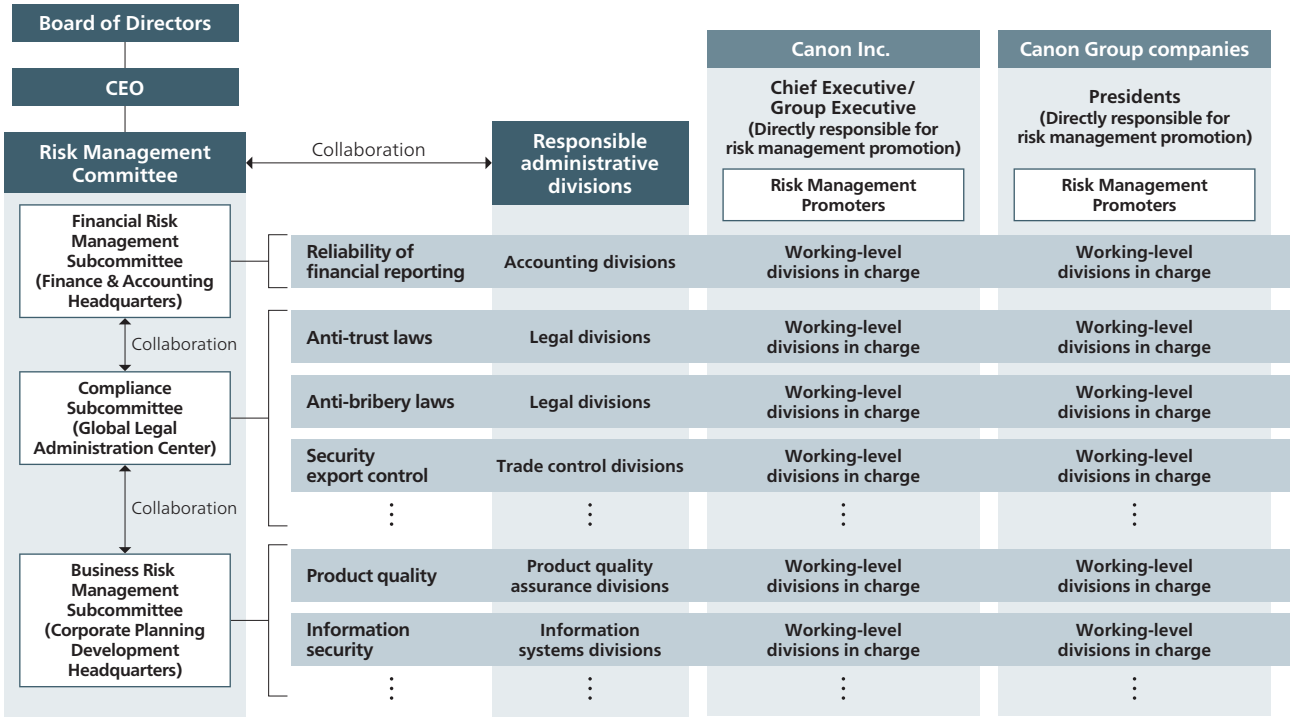
The Risk Management Committee develops various measures with regard to improving the Canon Group's risk management system, including grasping any significant risks (violation of laws and regulations, inappropriate financial reporting, quality issues and information leakage, etc.) that the Canon Group may face in the course of business. Additionally, in accordance with the Group's annual plan approved by the Board of Directors, the Risk Management Committee evaluates the status of improvement and implementation of the risk management system and reports its findings to the CEO and the Board of Directors.

Heads of Canon Inc. divisions and presidents of Canon Group companies, as those responsible for promoting risk management, formulate an individual annual plan for each division and Group company based on the Group's annual plan, and bear the responsibility of improving their risk management system. Risk management promoters appointed for each division and Group company coordinate related risk management practices. Canon Inc. administrative divisions with jurisdiction of miscellaneous risks associated with the company's

Improvement and Implementation Processes of Risk Management System



Risk Management Promotion System



business activities, including legal division, security trade control division, and quality assurance division, monitor and provide assistance for the improvement of risk management systems by each Canon Inc. division and Canon Group company.

Financial Risk Management

The Financial Risk Management Subcommittee carries out activities for strengthening 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.

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 2015.

Compliance

The Compliance Subcommittee works on promoting corporate ethics in accordance with the Canon Group Code of Conduct, and on improving the group's legal risk management system.

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 global 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

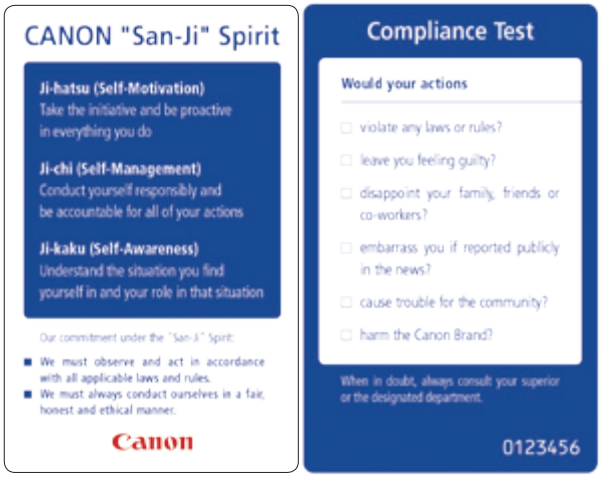
1. Compliance with Corporate Ethics and Laws
   • Fairness and sincerity • Legal compliance in performance of duties • Appropriate interpretation of applicable laws, regulations and company rules
2. Management of Corporate Assets and Property
   • Strict management of assets and property • Prohibition 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. This set of principles clarifies the Canon Group's management stance and standards that Canon Group executives and employees must comply with in their duties. In addition to Japanese, the Code of Conduct has been translated into 14 languages, including English, French and Chinese, and approved by resolution of the Board of Directors of each Canon 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 as well as 16 other languages, including English, French and Chinese, and given out to all executives and employees. 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 is a compliance test that enables employees to carry out self-questioning of their actions on a daily basis.



Compliance Card

Corporate Ethics and Compliance Training

Canon Group companies both inside and outside of Japan carry out corporate ethics and compliance training for employees based on the circumstances and conditions of the region where they operate.

For example, Canon Inc. conducts compliance training designed to foster compliance awareness for newly appointed general managers and managers, new employees as well as management level employees of specific organizations and Group companies.

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.

Whistleblower System

At Canon Inc., we have a hotline in place to receive information related to issues of compliance. The confidentiality of callers is strictly maintained, and callers are guaranteed not to suffer detriment for using the hotline. We continually work to improve the system to encourage use by raising awareness of the hotline services, using such means as an intranet compliance site and compliance training.

Hotlines have been established at nearly all Group companies worldwide. Canon Inc. and Group companies' divisions in charge are in close coordination to continuously respond to incoming reports and increase system reliability.

Legal Risk Management System

At Canon, we have identified significant legal risks that the Canon Group may face in the course of business (e.g. violations of anti-trust laws, anti-bribery laws and export control regulations) by considering potential likelihood and impacts on Canon's business. To minimize these risks, we are working to establish a system to ensure legal compliance by improving operational workflows and rules, providing training on laws for relevant employees, and conducting audits and checks.

Thorough Compliance with Export Control Regulations

At Canon Inc., we have established a security trade control framework headed by the president and controlled by the Foreign Trade Legal Division within the Global Logistics Management Center. This ensures that we can implement proper security trade controls in compliance with strict regulations on the export of commodities and technologies for civil use that could be diverted for use in weapons of mass destruction or conventional weaponry.

The Foreign Trade Legal Division works with divisions involved with individual commodities and technologies to double-check such issues as whether commodities and technologies for export are controlled by regulations, or whether trading parties are engaged in the development of weapons of mass destruction. We have also established and revised the Security Trade Control Guidelines, and hold regular briefings and training sessions for persons in charge of Canon Inc. business divisions and Group companies in Japan to further educate employee about the importance of security trade control. We also provide Group companies with templates for company rules, training curriculum for employees, and support via the help desk to help these companies put a control framework and rules in place.

Such thorough internal controls have ensured that the Canon Group has never violated laws concerning security trade control. Canon Inc. has also maintained a bulk export license from Japan's Ministry of Economy, Trade and Industry continuously since 1990. This license is granted only to exporters who exercise strict controls.

Liaison meeting on security trade control involving Group companies

Compliance with Anti-trust Laws

Anti-trust laws apply to all of Canon's business activities, from product development to production, sales and after-sales service, and therefore, Canon recognizes that compliance with these laws is absolutely vital.

Based on this awareness, business divisions of Canon Inc. and sales and service companies of the Canon Group conduct regular training for employees of divisions exposed to the risk of anti-trust law violations to educate them about the laws, provide examples of legal violations, and give them things to look out for in their duties. We also make our anti-trust law hotline known to all employees and thoroughly encourage employees to use this hotline if they are unsure of how to interpret or apply anti-trust laws.

Prevention of Bribery

The Canon Group Code of Conduct clearly stipulates that Canon will not receive benefits in the form of gifts or entertainment that exceed the social norm, or provide similar benefits to other parties.

Canon Inc. and its Group companies inside and outside Japan carry out regular training for employees of divisions involved with negotiations between public officials and business partners to inform them about the latest regulatory trends in major countries and details of the Code of Conduct.

Business Risk Management

The Business Risk Management Subcommittee is responsible for operational risks excluding legal violations and errors in financial reporting.

Individual risks are assigned to the divisions in charge for the entire Canon Group. The Business Risk Management Subcommittee works with working-level divisions in charge from each Canon Inc. organization and Canon Group company to carry out risk mitigation activities and further improve the risk management system.

Information Security

Recognizing that information security is a vital management task, Canon has established an appropriate management system for the entire Group. Under this system, we carry out training to raise employee awareness and to prevent external threats and leaks of confidential internal information.

Management Structure

Canon has established the Information Security Committee as a decision-making body for information-security measures. This committee is made up of experts from information security departments and is responsible for the information security management of the entire Group.

Committee members have also drawn up the Canon Group Information Security Rules in order to maintain the same level of and approach to information security across the entire company. These rules apply to all Group companies worldwide. Each Group company creates regulations and guidelines based on these rules that are in line with its needs, and then carries out training and promotional activities.

Information-security check at a Canon Group company

Based on these rules, regional marketing headquarters conduct regular inspections to confirm how information security is being implemented at each Group company, using the data to review and improve information security controls.

If an information-security incident occurs, the matter must be reported to the Information Security Committee via the respective regional marketing headquarters. In turn, the committee will issue instructions based on the details of the incident.

CSIRT*, a dedicated team for dealing with growing information network threats, was established within Canon Inc. in 2015. At the same time, Canon officially joined the Nippon CSIRT Association as Canon-CSIRT in order to address the increasingly sophisticated nature of cyber attacks by reinforcing collaboration with outside CSIRTs.

Additionally, Canon Inc.'s Information & Communication Systems Headquarters carried out information-security checks on 28 Group companies in Japan and 22 Group companies overseas. These inspections found that each company's system was sound and in good working order.

Canon will maintain an expedient and smooth communication channel with its Group companies and make every effort to ensure that its mechanisms can identify and remedy issues based on regular information security checks. Moreover, we are also working to further reinforce our information security system by establishing a structure to discover information-security incidents at an early stage and measures to eliminate security leaks and risks connected to these incidents.

* CSIRT stands for Computer Security Incident Response Team. This is a dedicated organization that deals with incidents involving computer security.

Preventing Information Leakage

Canon implements measures that safeguard the three elements of information security, namely, confidentiality*1, integrity*2, and availability*3 of corporate information.

Valuable information is stored using a specialized system with reinforced security. By controlling access and recording usage, we guard against external attacks and prevent internal information leaks.

In addition, Canon has established an environment in which employees can safely access their company's information assets while away on a business trip, and has also placed restrictions on email attachments and taking company computers or recording media offsite.

To safeguard against the threat of external attacks, we carry out training and other measures to prevent the illegal modification of Canon's official websites and deal with targeted email attacks.

In 2015, we continued on with these efforts while also working to prevent email viruses and spam mails (through stopping transmissions and isolating received email) and introducing automatic encryption of file attachments when an email is sent externally, in an effort to further enhance security and protect against the threat of information leakages. Going forward, we will continue to work on improving our countermeasures to maintain the three elements.

*1 **Confidentiality**
Enable only authorized personnel to access information.
*2 **Integrity**
Ensure data and processing methods are accurate and cannot be modified without authorization.
*3 **Availability**
Make data accessible to authorized personnel when needed.

Protecting Personal Information

Canon recognizes that personal information is an important asset, and that protecting this asset is one of its social responsibilities.

At Canon Inc., we have created rules to safeguard personal information, including the Personal Information Protection Policy and Personal Information Protection Rules, and conduct training and audits regularly as part of our system to prevent leakages 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 Canon Group. As a result, once again there were no incidents involving the loss or leakage of personal information at Canon Inc. or any of its Group companies in 2015.

In addition, Canon Group companies in Japan formulated the My Number Handling Rules and My Number Regulations in order to manage Japan's new Social Security and Tax Number System (referred to as the "My Number" system) in an appropriate manner.

Going forward, we will regularly monitor our management of personal information and the My Number system while also reviewing operations to make appropriate changes as needed.

Information-security Training

In order to maintain and improve information security, Canon is focusing on raising awareness among those accessing information systems, namely, employees.

New employees are thoroughly trained on Canon's information-security measures and rules through group training held for both regular and mid-career hires. In addition, training is provided annually for all employees, including temporary employees, using our e-learning system.

In 2015, roughly 28,000 employees—the equivalent of Canon Inc.'s total workforce—received information-security training. The training curriculum focused on reaffirming the importance of various measures related to information security. This included how to respond to a targeted email attack and what to look out for when sending email or when using information infrastructure, such as the risk of information leakages from posting on external translation websites.

Canon is committed to improving the content of its training programs in order to raise employee understanding and awareness of information-security matters.

Physical Security

Aiming to strengthen physical security, Canon has been working to establish physical-security systems at each of its operational sites based on the following three policies:

1. Establish and put into practice at operational sites an overall design from the viewpoint of disaster prevention, crime prevention, and safety to optimize entry and exit routes for all persons.
2. Fully implement strict internal and external security measures to comprehensively prevent company assets (physical objects, information, etc.) from being removed, suspicious objects from being brought in, and suspicious individuals from entering.
3. Limit entry to certain areas to people who have been authorized by area managers, and integrate management of room entry and exit logs.

Physical Security Promotion System

Canon established the Canon Security Guidelines, which outlines the policies and rules regarding room entry and exit management and other kinds of physical security. We have since then been actively promoting security measures according to these guidelines, while also making revisions to these guidelines as needed. Each Canon site is now responsible for drafting a self-checklist that complies with the guidelines and also takes into account the unique security risks of each region in order to check the level of their security protocols. In this way, each site implements security measures tailored to

changes in their own environment.

In addition to the Integrated Entry and Exit Management System, a control system that comprehensively manages surveillance cameras and various sensors has been implemented as part of Canon's efforts to strengthen physical security across the entire Group.

Due to the serious risk to society posed by toxic materials, we have developed a particularly thorough audit system, covering all Canon Group sites in Japan. Improvements and revisions to physical security measures are implemented based on the results of these audits.

Learning from the terrorist incidents in Paris and Belgium, Canon has stepped up its security efforts in order to quickly detect suspicious persons and suspicious objects for the purpose of preventing indiscriminate terrorist attacks against companies, which are considered a soft target. And, we are working more closely with the police, fire department and other government agencies to heighten vigilance against possible attacks.

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 even after a natural disaster or emergency represents one of the most important social responsibilities of any company. It is based on this recognition that we have formulated a business continuity plan (BCP) *1 and the Canon Group Disaster Preparedness Guidelines, and we 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 the Disaster Recovery Center*2 to back up information systems to ensure that the mainframe system will operate securely in the event of a disaster.

We have also updated all Group company facilities, setting up emergency communications equipment and support structures, and inculcated a sense of readiness in our employees through practical disaster-preparedness training.

Furthermore, we have prepared a manual for persons in charge 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.

In 2014, we established a system for conducting communications training involving the headquarters, business sites and Group companies once every month using satellite telephones to prepare for the potential interruption or shutdown of communications infrastructure. The Disaster Provision Standards were also drawn up following the enactment of the Tokyo Metropolitan Ordinance on Measures for Stranded Persons.

In 2015, we continued to conduct the above-mentioned communications training and carried out a training exercise to set up a disaster recovery countermeasure headquarters at our Shimomaruko headquarters based on the scenario of a large-scale natural disaster. Also, we moved forward with the stocking of non-food provisions, including blankets and disaster toilets based on the Disaster Provision Standards.

Evacuation training at our Shimomaruko headquarters

*1 **Business continuity plan (BCP)**
A business continuity plan is an action plan that includes measures to provide for the continuation of a minimal level of business in the event of fire, 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.

Revisions to the Disaster Agreement with Ota Ward, Tokyo

Canon Inc. has concluded a disaster agreement with Ota Ward, Tokyo, where its Shimomaruko headquarters is located. In 2015, at the request of the Disaster Prevention Section of Ota Ward, we revised the agreement so that our newest facilities, including a lecture hall, gymnasium and heliport, can be offered in the case of an emergency situation.

Going forward, we will continue to work closely with local governments to fill the role of a disaster-response base in the local community.