

Corporate Governance

To increase corporate value, Casio always strives to improve management integrity and transparency. True to this commitment, Casio works to ensure that management decision-making is quick and that all operations are executed properly and efficiently.

Corporate Governance Framework

Casio recognizes that quick decision-making, proper execution of operations, and a robust management oversight function that increases the integrity and transparency of business management are extremely important factors in achieving business goals and continuing to raise corporate value. This recognition guides Casio's ongoing efforts to improve corporate governance.

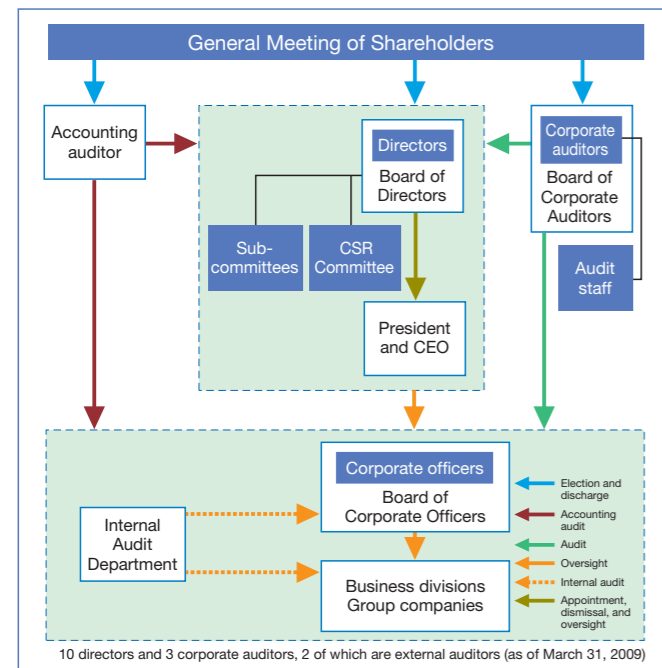
In June 1999, Casio adopted a corporate officer system that clearly separates the management oversight and execution functions. Meetings of the board of corporate officers are attended by corporate officers, directors and corporate auditors. They deliberate on important affairs relating to the execution of business operations, and this mechanism enables implementation of group-wide adjustments and measures.

The board of directors is tasked with making prompt, reasonable management decisions. Board meetings are attended by directors and corporate auditors, who discuss and make decisions on important business issues. Furthermore, in order to clarify the management responsibility of directors and to ensure a prompt response to changes in the business environment, the term of office of directors was changed from two years to one, as of June 2007.

In accordance with audit policies approved by the board of corporate auditors, corporate auditors (including external auditors) attend board of directors' meetings, meetings of the corporate officers, and other important meetings. In addition, they perform careful audits by gathering information and receiving reports from directors and others, and by reviewing resolution documents relating to important decisions.

Accounting auditors perform external audits according to generally accepted Japanese auditing standards, and they also provide recommendations for operational improvement. The Internal Audit Department carries out audits of Casio operations to ensure they are in conformity with laws and regulations as well as internal standards such as the Organization Control Standard.

Corporate governance framework



It also conducts evaluations and offers recommendations for improvement.

Casio also has a CSR Committee consisting of the directors and corporate auditors, which is chaired by the president of Casio Computer Co., Ltd. It discusses basic policies and vital matters related to group-wide CSR activities.

System of Internal Control

Japan's new Financial Instruments and Exchange Law has mandated the establishment of internal control reporting systems* effective from the fiscal year ending March 31, 2009. Accordingly, Casio has established basic policies to ensure the accuracy and reliability of its financial reporting. It has also set up an Internal Control Committee composed of members of the Accounting Department, Information System Department, CSR Operations Section, and Internal Audit Department, in order to secure an effective internal control system.

In fiscal 2008, documentation of important business processes was carried out according to standard guidelines applying to the entire group. In fiscal 2009, a monitoring system and rules were established in order to identify risks that can impact financial reporting in the key business processes of main departments and group companies at an early stage. Each Casio site carries out self inspections to check whether operations are being performed according to documentation, and the results are regularly reported to the Internal Control Committee.

The Internal Audit Department, which is independent of the business divisions, also evaluates the internal control establishment and operation conditions, based on group-wide evaluation standards.

Through the activities outlined above, Casio checks that each site is always carrying out its operations in a proper manner. Whenever problems or inefficiencies are discovered during this process, improvement plans are prepared and implemented based on consistent policies of the Internal Control Committee.

Going beyond the formal steps required by the law, Casio has been constructing internal controls with real effectiveness and taking advantage of the opportunity to improve operations. The company is establishing and executing methods and rules on its own initiative. This included evaluation and improvements in fiscal 2008 based on process documentation performed in fiscal 2007.

The entire group will continue making quality improvements to its internal control system from fiscal 2010 onward, through improvements and continuous implementation of the aforementioned activities.

* A system required for listed companies under Japan's Financial Instruments and Exchange Law, effective from the fiscal year ending March 31, 2009, intended to secure the reliability of financial reporting. Each company evaluates its own internal controls, and then is audited by external auditors, before submitting an internal control report to the prime minister of Japan.

For more details on corporate governance, visit the following site. Corporate Governance Reports (Tokyo Stock Exchange: Search for Corporate Governance Information)

URL <http://www.tse.or.jp/english/rules/cg/index.html>

Compliance and Risk Management

The Charter of Creativity for Casio, the Casio Common Commitment, and the Casio Code of Conduct form the foundation that governs the behavior of all Casio employees. Casio has also established a risk management system and Whistleblower Hotline. This three-in-one approach represents a robust means of ensuring compliance.

Casio Group Code of Conduct

The Casio Group Code of Conduct represents a promise from all of Casio's directors and employees to observe relevant laws and ethical standards during the execution of their occupational duties, and also in their daily lives, as responsible members of society.

Casio made changes to the Code of Conduct in May 2008 to reflect revisions in Japanese law and meet society's changing expectations, also taking the chance to improve the precision of the document. The scope of applicability was clarified, additions and revisions were made to the conduct items, and items were put in order of priority.

With this major revision of the Code, it was given a new name to include all the companies of the Casio Group, worldwide. Japanese and English versions of the code were prepared to serve as the basis for translation into other languages by individual group companies, encouraging full understanding among all group employees.

To promote awareness of the newly revised Casio Group Code of Conduct, special training sessions were carried out at group companies in Japan, and a compliance questionnaire was conducted on topics including the Whistleblower Hotline and the Charter of Creativity for Casio and Casio Common Commitment. The questionnaire results were analyzed by the Risk Management Committee Secretariat, and issues were identified by topic. Each of these issues will be reflected in an action plan for fiscal 2010.

Provisions of the Casio Group Code of Conduct

1. Purpose
2. Basic Policies
3. Code of Conduct
 - 3-1. Compliance with Laws and Ethics
 - 3-2. Respect for Human Rights
 - 3-3. Provision of Safety and Peace of Mind to Customers
 - 3-4. Fair Competition and Transactions
 - 3-5. Separation of Personal Affairs from Business
 - 3-6. Information Protection
 - 3-7. Environmental Conservation
 - 3-8. Disclosure of Corporate Information
 - 3-9. Maintenance of Social Order
 - 3-10. Social Contributions
4. Implementation of the Code of Conduct
5. Handling Violations

Risk Management

In May 2006, Casio established Basic Risk Management Policies, building a solid risk management organization designed to efficiently manage risk.

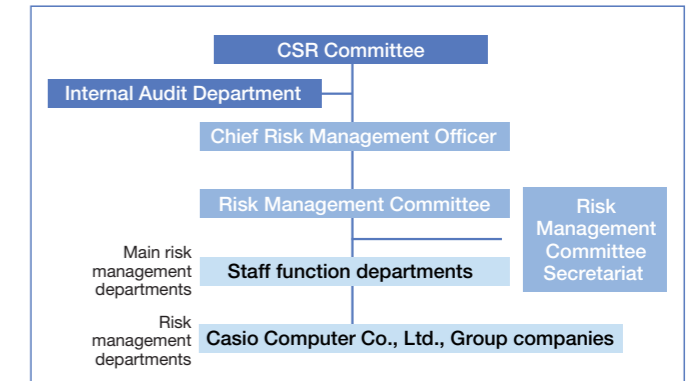
Specifically, a Risk Management Committee chaired by the Chief Risk Management Officer has been established under the CSR Committee. The Risk Management Committee discusses and makes decisions for selecting and addressing important risk management issues.

The main risk management departments are the internal staff function departments. They proactively carry out measures to address risk management issues, and raise awareness among relevant departments in the group.

The Risk Management Committee Secretariat operates a management system based on the plan-do-check-act (PDCA) cycle, and oversees the progress of risk management activities.

The Internal Audit Department performs audits of this management system, independently from the risk management activities.

Risk management system



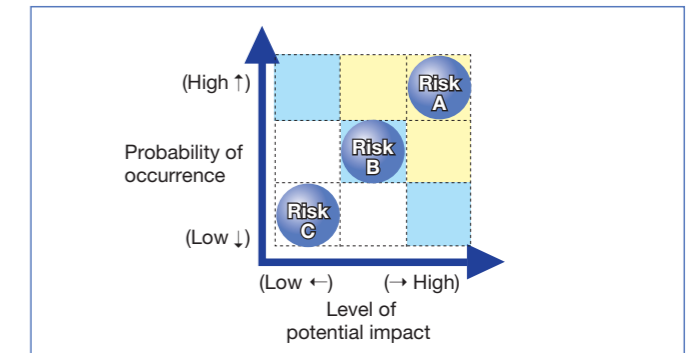
Fiscal 2009 Activities

The following is a report on risk management activities undertaken in fiscal 2009, according to the PDCA cycle.

Selection of Risk Management Themes Plan

Continuing from the previous year, the risk management themes selected for fiscal 2009 had to do with compliance. However, after evaluating the selection method used the previous year, in order to identify risks more objectively, detailed standards regarding the level of potential risk impact were established. Consequently, objectivity was increased for the analysis and evaluation of risk based on both potential impact and probability of occurrence, and good results were achieved for evaluation consistency.

Risk prioritization using probability of risk occurrence and level of potential impact



The Risk Management Committee Secretariat performed analysis and evaluation, and exchanged opinions with in-house experts on identified risks. Upon approval from the CSR Committee, the risk management themes for fiscal 2009 were determined by the Risk Management Committee. At the same time, measures were divided into the categories of "highest priority" and "priority," according to the degree of urgency. A total of 20 risk management themes were addressed in fiscal 2009, along with issues where targets had not been achieved in the previous year.

Risk Management Activities Do

The main risk management departments prepare annual risk management programs on each of the risk management themes, and promote individual risk prevention measures according to the program schedule. Along with the establishment of new timeframes for achieving targets for themes not achieved in fiscal 2008, the departments promoted improvements on unsatisfactory items indicated in internal audits, and worked hard to quickly reach targets. On these activities, the secretariat performed progress checks once every quarter. Risk Management Committee meetings were held twice during the year, where policies and goals were confirmed, progress made on individual risk management themes was announced, and the overall level of progress was verified.

Evaluation of Risk Management Activities Check

At the end of the fiscal year, the secretariat carried out a performance evaluation and a system effectiveness evaluation for risk prevention measures promoted by the main risk management departments. The departments first used a prescribed evaluation sheet to determine whether their risk management activities on each theme were carried out according to the initial plan, and whether their systems functioned effectively. The results were then sent to the secretariat for evaluation.

After the evaluation was complete, the Internal Audit Department performed an audit. This audit focused primarily on whether management systems had been properly implemented, maintained and operated.

The secretariat also performed monitoring of risk management themes where targets had been achieved in fiscal 2008, while confirming status of progress on an ongoing basis.

Review of Risk Management Activities Act

Audit results are reported to top management, along with the secretariat's evaluations of performance and system effectiveness. Top management reviews these evaluation results and issues the necessary instructions for improvement with regard to risk management activities or management systems. There were no significant instructions required after the fiscal 2009 management review.

Thanks to this management cycle, in fiscal 2009 positive results were obtained in the internal audit by the audit department and in the evaluation by the secretariat. Initial targets were achieved for 14 themes.

The remaining 6 themes will be addressed as continuing risk management issues in fiscal 2010, through ongoing activities.

Responding to Emergencies

The environment in which companies operate presents a variety of risks, and responding to incidents quickly and flexibly is a crucial aspect of business management. In the event of an emergency, saving human life takes first priority, and this requires an initial response that is both rapid and appropriate.

In order to respond to these contingencies with the resources of the company organization, Casio has created a Crisis Management Manual for securing the safety of all employees, directors, and their families, preserving corporate assets, and maintaining business activities.

Sequential updates of the manual keep pace with changes in the business environment, and the company is taking practical initiatives at the same time. Specifically, the following measures have already been undertaken:

- Evacuation drills for employees
- Development and in-house distribution of disaster prevention support tools
- Construction of a system to ensure absolutely no contact with organized criminal elements
- Disaster prevention drills and disaster stockpiling in cooperation with local communities.

In addition, an action plan to prepare for an influenza pandemic has been set as a priority issue, and Casio is striving to improve its overall crisis management and response capabilities.



In 2008, the Hatsudai Headquarters of Casio Computer Co., Ltd., set up an aid station as part of the "Coordinated Practice for Walking Home after a Disaster in the National Capital," sponsored by the Tokyo Volunteer Network for Disaster Relief.

Information Security

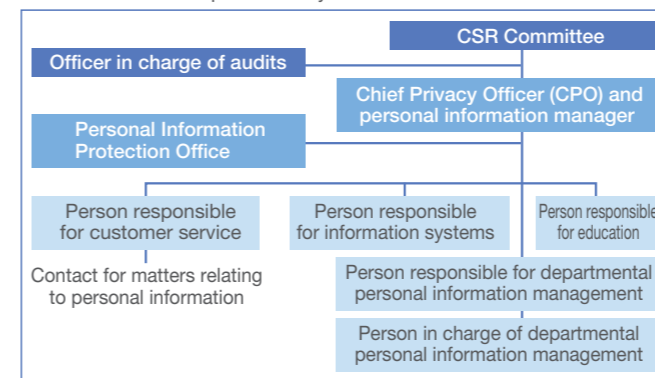
Casio is aware of its important social responsibility to maintain the security of information that it collects from customers and other stakeholders in relation to its business activities. Casio strives to maintain the highest level of information security. With the full implementation of Japan's Act on the Protection of Personal Information, Casio launched the Protection of Personal Data Project. Furthermore, as part of Casio's drive to strengthen its system for safe and proper handling of personal data, Casio Computer Co., Ltd., worked to qualify for the Privacy Mark* certification and received it in December 2005. Since obtaining certification, Casio has been properly carrying out the plan-do-check-act (PDCA) cycle to maintain its personal information protection management system. Along with the revision of JIS Q 15001 in May 2006, the company revised its applicable rules, and worked to strengthen supervision of information consignees, receiving renewed certification in March 2008.

In fiscal 2009, these personal information protection activities were expanded from Casio Computer Co., Ltd., to other group companies, as part of efforts to strengthen internal controls. Casio promoted the same system for personal information protection used at the parent company, focusing on group companies that handle large volumes of personal information. Going forward, Casio will keep strengthening information security and personal information protection throughout the group to further increase stakeholder confidence.



* A program where the Japan Information Processing Development Corporation, a public-service foundation, evaluates the adequacy of corporate protective measures related to the handling of personal data. Companies that are found to have adequate protective measures in place are certified and permitted to display the Privacy Mark.

Personal information protection system



Employee Message

Since Japan's Personal Information Protection Law came into effect, every day the newspapers have stories about companies mishandling or leaking personal information. Most of these cases are due to small oversights or errors on the part of employees.

In order to prevent such incidents at Casio, we emphasize raising the awareness of all employees, and everyone in the Personal Information Protection Office is working together to strengthen our information protection systems, focusing on training and awareness campaigns.



Rie Sato
Personal Information Protection Office

Whistleblower Hotline

As way to help ensure compliance, Casio set up a Whistleblower Hotline in April 2006. The hotline has been functioning with neutrality and fairness across all of its internal and external contact points. The goal is to prevent risks from developing into real problems, and the Hotline Office responds to all calls and requests for consultation, working hard to counter any improper behavior.

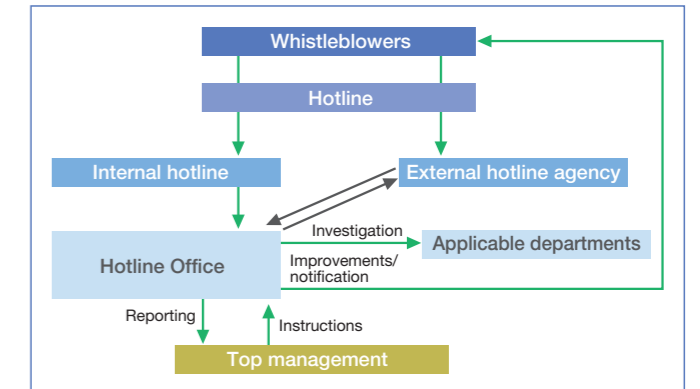
In fiscal 2009, 13 calls were made to the hotline, about half the number in the previous year.

Employees that were the subject of hotline reports were given training and guidance along with proper treatment based on internal rules, as part of efforts to prevent reoccurrence.

In fiscal 2009 a Whistleblower Hotline questionnaire was given to group employees in Japan. Specific issues were identified from the results, and will be reflected in future operations.



Whistleblower Hotline



Export Control

In 1987, Casio Computer Co., Ltd., established the Export Control Security Program of Casio Computer Co., Ltd. (a compliance program) in order to make sure proper measures are taken to ensure the security of exports, thus helping to maintain international peace and security. The program has since been continually updated along with changes in the Japanese Export Control Regulation.

Casio has appointed employees responsible for export control in relevant departments as part of an internal system to ensure observance of the program.

As relevant regulations are revised, the needed training updates have been given to the employees responsible for export control. Casio is committed to total legal compliance, and ensures that the program is properly maintained and managed through annual self-audits.