



# Governance Structure

## Themes of activities in fiscal 2008

In fiscal 2008, our governance activities were again centered on two themes: advancing CSR activities in the NEC Fielding Group, and continually enhancing our activities aimed at Zero Risk.

## Results of activities in fiscal 2008

In fiscal 2008, we took steps for functional reinforcement of the Crisis Management Committee under our activities aimed at Zero Risk. In addition to the business continuity plan (BCP) prepared on the premise of occurrence of natural disaster, we also commenced formulation of a BCP premised on the outbreak of H1N1 influenza.

## Future challenges

As for tasks in fiscal 2009, we see a need for efforts to bolster governance throughout the NEC Fielding Group. To this end, we are taking action to spread the Fielding Vision and Values among the group companies and lay down guidelines for CSR activities for promotion of the same by the Group as a whole.

## Setup of corporate governance\*

Our company has a board of directors and a board of corporate auditors. We also introduced a scheme of corporate officers, in order to ensure swifter decision-making and more efficient supervisory and monitoring functions of the board of directors.

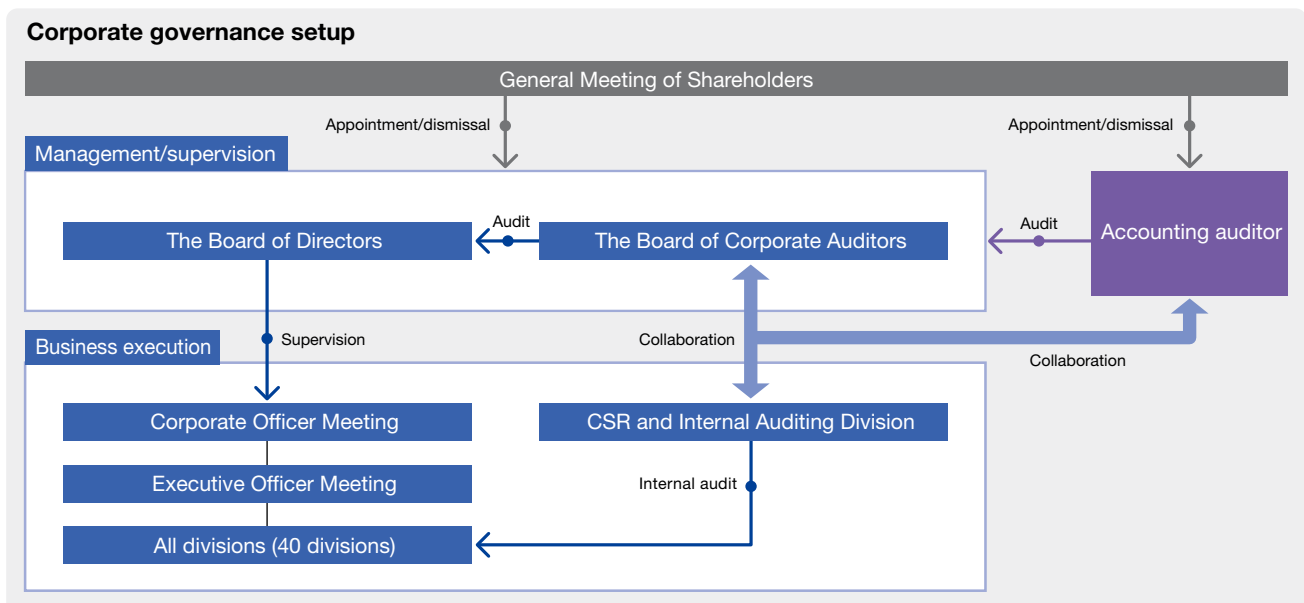
The board of directors holds provisional meetings when needed as well as regular monthly meetings. It reviews and discusses important issues prior to meetings, thus enabling more flexible and appropriate management decisions. In addition, to clarify the management responsibilities, the tenure of directors is limited to one year.

The board of corporate auditors, on the one hand, meets six times a year. Our corporate auditors and an accounting auditor (KPMG AZSA & Co.), as well as our internal audit division (CSR and Internal Auditing Division) work in close collaboration with each other, through exchange of information related to audit activities as needed.

\* **Corporate governance** : A framework for monitoring corporate management. Specifically, it has functions to monitor the management who are committed to manage their company with the goal of maximizing shareholders interest. These functions include setting targets for the management, evaluating and monitoring their performance to produce reasonable shareholders value.

## Ensuring corporate governance of subsidiaries

We send directors and corporate auditors to our subsidiaries, and provide guidance and support in creating a legal-compliance framework, in order to ensure corporate governance of our subsidiaries. Our internal audit division (CSR and Internal Auditing Division) also audits our subsidiaries, providing guidance and recommendations for improvements as necessary.



## Constructing an internal control\* system

We have established an internal control system, which consists of various types of systems such as a risk management system and information security system, under our Basic Policy on Construction of the Internal Control System determined in accordance with Article 362, Paragraph 5 of the Companies Act of Japan.

\* Internal control : Please refer to page 15.

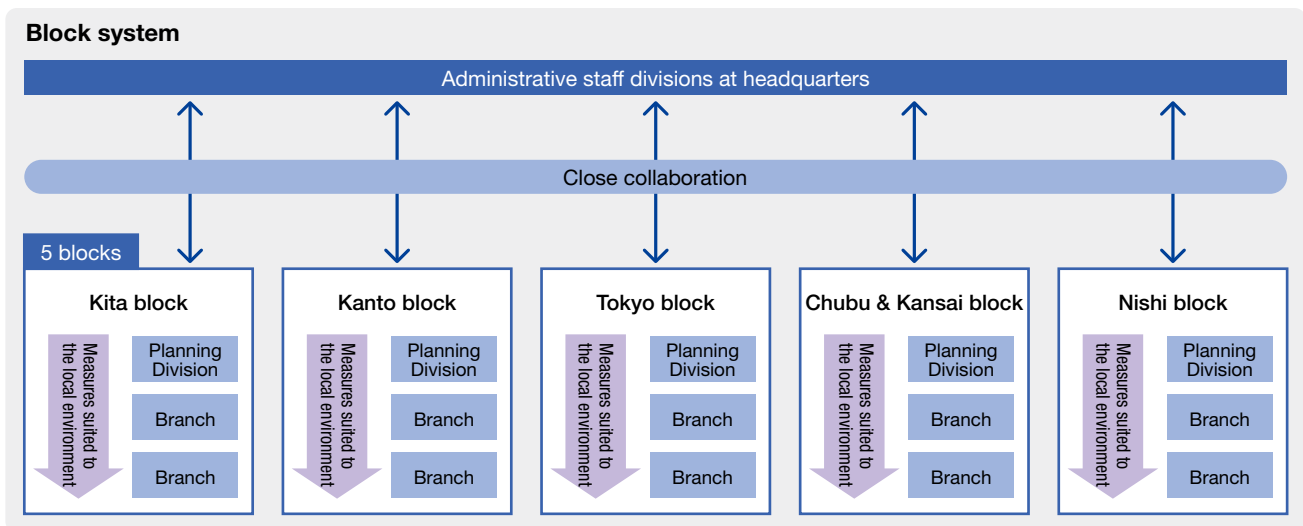
### Basic Policy on Construction of the Internal Control System

Pursuant to Article 362, Paragraph 5 of the Companies Act of Japan, we have determined the following basic policy with respect to systems (internal control systems) set forth in Article 362, Paragraph 4, Item 6 of the Companies Act, as well as in Article 100, Paragraphs 1 and 3 of the Ordinance for Enforcement of the Companies Act. Under such basic policy, we ensure appropriateness of, and constantly review, improve, and enhance our business operations, according to changing conditions of social, economic, and other aspects in our business environment.

## Introduction of a block system

In October 2007, we introduced a block system for our business-line groups, aiming to create a more comprehensive structure extending beyond the boundaries between each branch. The block system centralizes administrative staff functions—once existing

at the branch level—into “blocks,” enabling operations to be performed faster and more efficiently, as well as enhancing governance by ensuring close collaboration with administrative staff divisions at headquarters.



## Creating a mutual supervision system by separating back-office operations

Back-office operations such as processing orders, sales, and payments were previously carried out at branches and sales offices. In order to establish a mutual supervision system, we have relocated all back-office works from sales locations to Business Compliance Centers (BC Centers) located in ten sites around Japan.

In fiscal 2008, we began shifting our operational system with local processing functions to a functionally integrated and centralized structure, thereby achieving the standardization of mutual supervision function across the Group.

### Roles of BC Centers

Stages	Roles
Posting of orders	Check order-processing information received from sales divisions in accordance with internal regulations as well as the Construction Industry Act and other regulations, and carry out processing of orders.
Processing of procurement	Place an order with subcontractors for specific services, or for appropriate goods from suppliers based on orders received, and carry out receiving checks.
Posting of sales	Check the delivery confirmation from customers, and carry out appropriate postings of sales.
Billing/ payments	Issue invoices to customers, and carry out a matching check with invoices to payments received.



## Approach to risk management\*

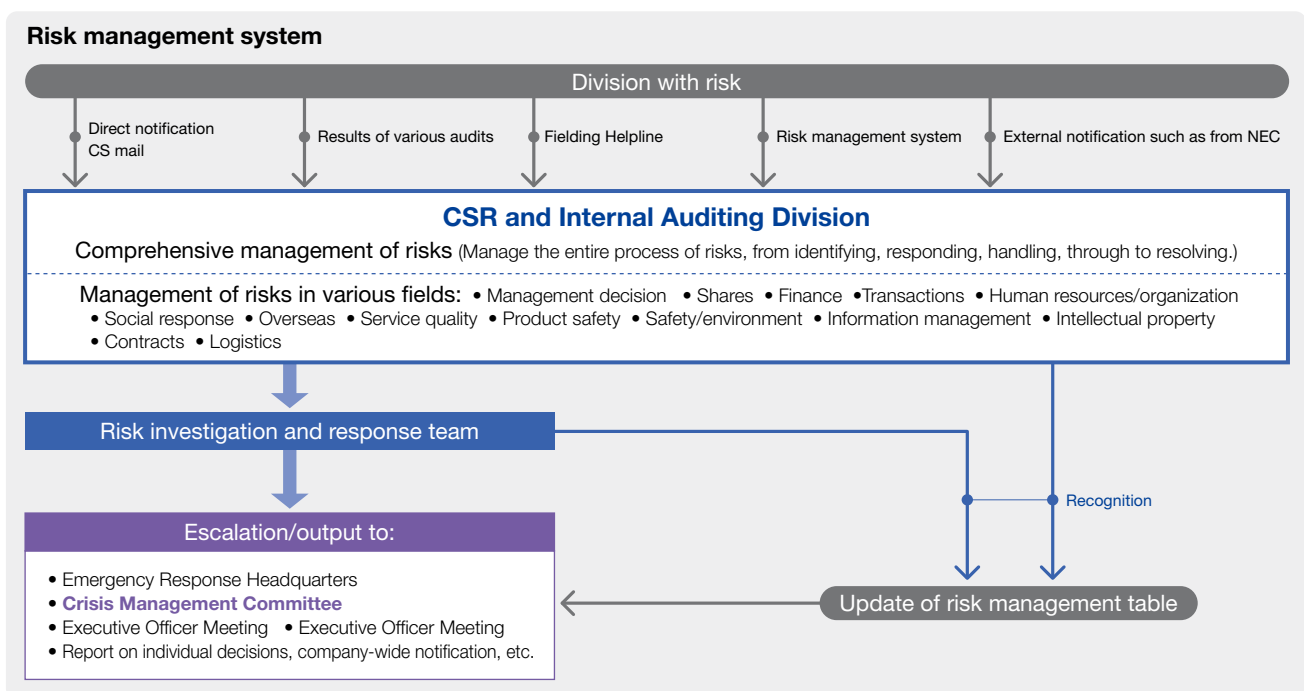
We are committed to swift and highly controlled risk management. We have created our Risk Management Basic Policy, and have built a risk-management system for our CSR and Internal Auditing Division to control overall risk.

\* **Risk management** : A process to manage risks systematically, and avoid or reduce losses and damages from risks. It is an operations-management methodology for effectively minimizing unforeseen damages from all types of threats, at the minimum cost.

### Risk Management Basic Policy

To avoid management crisis, we focus on the following initiatives:

1. Increase the degree of penetration of risk management and expand the risk management system;
2. Provide measures to follow up and reduce existing risks;
3. Identify new risks and provide measures to prevent them;
4. Decide divisions in charge of managing recognized risks and debate collateral measures (such as insurance); and
5. Conduct periodic risk assessments.



### Functional reinforcement of the Crisis Management Committee

In fiscal 2008, we reinforced the functions of the Crisis Management Committee. Previously, promotional meetings were convened separately for discussion and deliberation in each of the fields of information security, product safety, protection of personal information, and export management. To centralize risk information, we consolidated this work in the Crisis Management Committee. For more rigorous deployment of initiatives and risk information activities, we revised the Committee membership to allow participation by the representatives of each block on the business line as members.

This step rationalized and unified the participants, opportunities for reporting and consultation, and meeting output, and thereby accelerated the company-wide diffusion of CSR-minded management.

### Fiscal 2008 risk actualization and cases, and their handling

In fiscal 2008, risks were unfortunately actualized in forms such as information leakage due to mistaken e-mail and fax transmissions, and the loss of USB memory devices used in business.



In response, NEC Fielding took steps such as distributing stickers calling for prevention of mistaken fax transmissions to all of its locations. As in fiscal 2007, we also carried out programs of Internet education related to information security for all employees. In addition, we asked all employees to check for and delete any corporate business information on their personal-use computers and all IT equipment (CDs, USB memories, etc.), and collected pledges from them to the effect that they will not use their own private equipment for business.

## Approach to business continuity plans (BCPs)\*

Since fiscal 2006, we have been committed to establish our Business Continuity Plans (BCPs) in order to swiftly resume business operations in case of a major natural disaster, and keep providing necessary services for stable operation of lifeline. In fiscal 2008, we conducted several business-continuity trainings to prepare for a major earthquake, and also launched a new BCP in case of a new influenza pandemic.

\* **Business continuity plan (BCP)** : A plan (document) indicating policies and procedures for ensuring the continuity of the companies business in the event of natural disasters, terrorism, or other unforeseen events.

### Basic Policy on BCP Creation for Disaster Response

1. Place the highest priority on checking the safety of employees and their family, providing aid and support, and preventing secondary disasters.
2. Create a system that allows the resumption of operations (\*1) on the following day after a disaster hits.
3. Create a system that allows the resumption of business (\*2) on the second day after a disaster hits.

\*1 Resumption of operations: resume minimal in-house operations, including receiving damage reports

\*2 Resumption of business: actively call on customers and fully resume business following the recovery of customer systems

### Basic Policy on Response to Pandemics

NEC Fielding established the following basic policy on response to H1N1 (highly virulent) influenza. Placing top priority on safeguarding the lives of our employees and others, the policy is also aimed at discharge of our social responsibilities.

1. Place top priority on assurance of the safety of lives and maintenance of health.
2. Continue with the work of supporting IT systems, which are used to maintain socioeconomic functions, upon implementation of maximum measures to assure employee safety.
3. Even for IT systems which have no connection with maintenance of socioeconomic functions, make a maximum effort to continue support; provided that, there may be cases to reduce or discontinue such support activities, depending on the pandemic situation.
4. Cooperate with assurance of safety in the local community.

## Business continuity training

We have begun business-continuity training sessions in order to verify the validity of our BCPs, and ensure that all divisions are aware of this plan.

We conducted the training in February 2008, envisioning a major earthquake centered in the Osaka region. We started by setting up a disaster headquarters following the earthquake, confirming the safety of employees, and confirming the state of damages at our customers' sites. The President and all directors and senior management below him attended, from the recovery of our work sites to the recovery of our customer systems. The exercise was conducted with all our business sites nationwide connected via teleconference and radio.

Moving forward, we plan to conduct training continuously, in order to attain further improvements in our BCPs reflecting the outcomes of the training.

## Response to the Iwate-Miyagi Nairiku Earthquake

In response to occurrence of the Iwate-Miyagi Nairiku Earthquake in June 2008, we set up a task force just fifteen minutes afterward and began confirming the safety of our employees and the damage status of customer systems.

Fortunately, the damage to equipment was mainly minor and did not require the dispatch of personnel from Tokyo or other places. Within the next three days, more than 89% of the affected equipment had been repaired.

### Safety confirmation system for personnel

In 2002, we completed development of our safety confirmation system for personnel. This system enables employees and their families to register via the Internet using personal computers or mobile phones, in order to enable us to quickly confirm the safety of our employees in times of disaster.



Safety confirmation system for personnel

The system was put to the test following the Niigata-Chuetsu-Oki Earthquake and Iwate-Miyagi Nairiku Earthquake. In each case, we were able to confirm the safety of all employees within the day of the earthquake, resuming operations on the next day and starting recovery of our customers' systems.

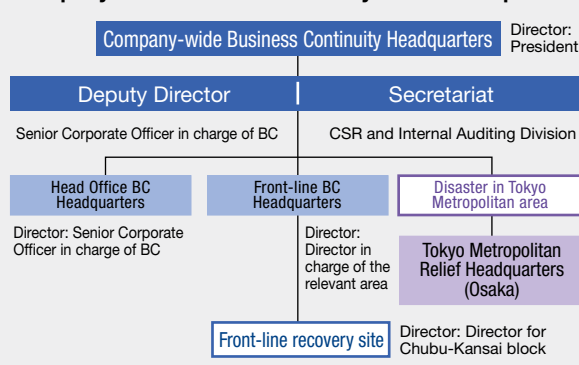
## Support for customer BCP response

We hold Fielding Solution Fairs across the country, where we give seminars on BCP, and provide information to raise our customers' awareness of business continuity planning. We also support our customers' BCP response through sales of CSR Supplies\*. Those include disaster-preparedness goods such as earthquake-proofing sheets that will keep IT equipment from falling over due to the shaking of an earthquake.

### Example goods for supporting customer BCP response

- Earthquake proof mat
- TCR seismic isolator
- Compact uninterruptible power system (UPS)
- Lightning arrester for communications lines

### Company-wide business continuity disaster-response



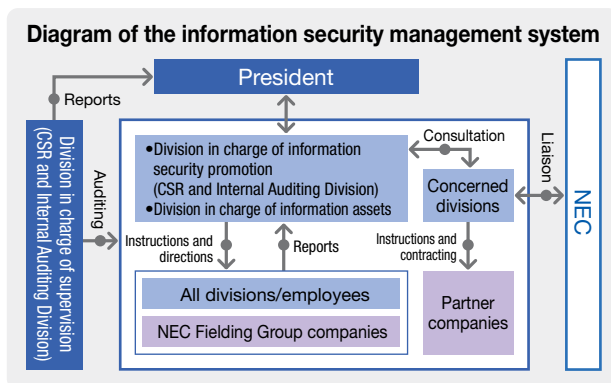
\* **CSR Supplies** : Products carried by NEC Fielding that assist our customers in environmental conservation or help reduce their risks. We aim to support our customers' CSR activities by promoting the sale of these supplies (e.g. recycled EP cartridges, backup power supplies, and earthquake-proofing goods).



## Approach to information security

We are often entrusted with customers' information assets while doing maintenance work for their information systems and network. Therefore, we consider risks related to information security and personal information protection as substantive CSR risks that need to be managed carefully, and continuously make efforts to eliminate them.

To prevent the occurrence of any accidents related to information security, we have established an information security management system based on our Information Security Basic Policy, thereby promoting prevention measures at the company-wide level.



## Information security measures

<ul style="list-style-type: none"> <li>• Install antitheft equipment on service cars</li> <li>• Install a safety box on service cars</li> </ul>	Antitheft measures
<ul style="list-style-type: none"> <li>• Install tools to prevent the HDD retrieval</li> <li>• Introduce PC-encryption software on all in-house computers</li> <li>• Expand the mail encryption method throughout the Company</li> <li>• Thoroughly introduce IRM*-based document protection</li> </ul>	Information leak countermeasures
<ul style="list-style-type: none"> <li>• Implement digital covenants and information security education</li> </ul>	Increase employee awareness

\* **Information Rights Management (IRM)** : A tool provided by Microsoft Office 2003 for preventing information leaks.

## Increasing employee awareness with a digital covenant

We strive to ensure that all employees at NEC Fielding, who often work at the offices of customers, are well aware of rules which they must abide by at these working sites. Such rules include maintaining information security they should be careful in daily work routines. In fiscal 2008, our employees again made a digital covenant that they fully understood the rules they had to adhere to, thereby raising thorough compliance awareness within the Company.

## Information Security Basic Policy

To protect the information assets entrusted to us by our customers and transaction partners as well as those of our own, and to contribute to socioeconomic advancement through supply of better goods and services, NEC Fielding has determined the following basic policy on information security, and hereby proclaims its commitment to practicing this policy.

1. We shall establish a setup for information security management and strive for proper management of information assets.
2. We shall instate and apply in-house rules in accordance with this basic policy.
3. We shall provide education required for assurance of information security.
4. We shall take appropriate human, organizational, and technical measures, and endeavor to prevent information assets from incurring improper access, leakage, alteration, loss/theft, destruction, hindrance to use, or other damage.
5. In the event of a security problem involving information assets, we shall immediately ascertain the cause and take action to curtail any damage to the minimum.
6. We shall observe all laws, agreements with customers, and social norms related to information security.
7. We shall constantly review the aforementioned activities and strive to improve them.

## Approach to protection of personal information

In 2001, we formulated our Personal Information Protection Policy. Since then, we have been working to protect personal information under the company-wide management system for personal information protection, which is supervised by the President. In each division, we appoint a person in charge of personal information protection as well as a person in charge of divisional promotion of personal information protection, in order to make all employees aware of personal information protection activities.

We have acquired the official certification of Privacy Mark (P mark) in 2002, and passed the renewal examination of the certificate in 2008.



## Diagram of the system for personal information protection

