Risk Management

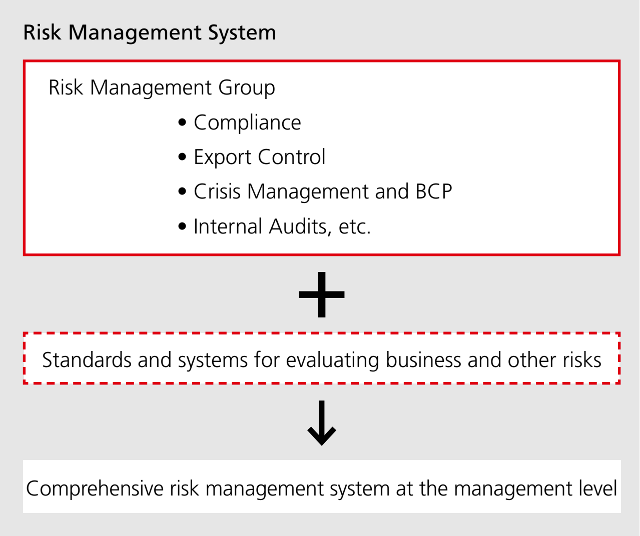
Changes to our operating environment from such factors as the globalization of the economy and advances in and spread of information and communications technology (ICT) not only lead to the expansion of business opportunities but also to the diversification of risks to our operations.

We have built a diverse risk management system under which we carry out risk analysis to accurately gauge ongoing economic and social changes and use the insights gained to take preventive measures and ensure a rapid response to issues that may arise unexpectedly.

Reinforcement of Risk Management System

The entire Hitachi Group is reinforcing its risk management system to address increasingly globalized and complexed risks.

Under Hitachi, Ltd.'s head of risk management, each business operation assigns an executive handling risk management to manage risks mainly concerned with compliance, export control, disasters, and crime, and to respond adequately in coordination among the entire Group. Furthermore, Hitachi is building a comprehensive risk management system that contains standards and procedures to objectively evaluate different risks that may affect business.



Risk Management System

Risk Management Group

- Compliance
- Export Control
- Crisis Management and BCP
- Internal Audits, etc.

+

Standards and systems for evaluating business and other risks

↓

Comprehensive risk management system at the management level

Creating BCPs* in Key Operations Worldwide

Given the close relation of our business to social infrastructure, we are enhancing our BCPs to ensure that the impact of risks does not disrupt our business and thereby significantly affect society. In December 2006, we issued the *Hitachi Group Guidelines for Developing Business Continuity Plans* in Japanese. In fiscal 2010 these were translated into English and Chinese for distribution to all Hitachi Group companies worldwide to ensure our response readiness for large disasters and other risks.

When the Great East Japan Earthquake struck in March 2011, our BCPs enabled quick responses and swift decision making. However, issues emerged including identification of secondary and other suppliers, cloud storage and multiplexing of production information, and the need to secure alternate transportation and fuel sources.

Based on the lessons learned from this disaster, in October 2011 we released and distributed new BCP guidelines for departmental implementation to further improve our BCPs. Hitachi Group operations in Japan completed their preparation and review of BCPs, based on applicability to their operations, by the end of fiscal 2011. BCPs for large earthquakes and novel strains of influenza have been prepared for 49 Hitachi, Ltd. business sites and 96 Group companies.

On top of these efforts, since fiscal 1998, Hitachi, Ltd. has held annual earthquake drills simulating a major seismic event at key operations in Japan. In November 2015, Hitachi Automotive Systems held coordinated drills at its head office and business sites in the cities of Sawa, Atsugi, and Fukushima, where managers in charge of their divisions confirmed the action plans in emergency situations based on BCPs.

In fiscal 2013, Hitachi appointed personnel in charge of risk-response policies at its main overseas bases and around 300 companies prepared BCPs with the goal of completing them for key operations by the end of fiscal 2013. These BCPs are aimed at strengthening our ability to respond to business risks, including large disasters, novel strains of influenza, political instability, and social disruption, as well as acts of terrorism. Moving forward, we intend to further expand the scope of our BCPs.

* BCP: Business Continuity Plan

Improving Safety for Employees Sent to Dangerous Regions

Responding to the hostage incident in Algeria in January 2013, then President Hiroaki Nakanishi reinforced his policy in February 2013 of ensuring the safety of employees sent outside Japan. Survey missions of in-house and outside experts are now sent beforehand to areas at high risk of war, terrorism, and other threats. Even after employees are dispatched to such areas, we conduct additional local surveys every six months as a means of confirming the effectiveness of our safety policies. In fiscal 2014, survey missions were sent to several countries in Africa and the Middle East. In addition, we have introduced a range of safety measures in the light of recent terrorist incidents involving Japanese and other nationals, including providing timely alerts to employees. These and other steps underscore our commitment to ensuring the safety of our employees working around the globe.

Hitachi is also contributing to safety measures at other Japanese corporations operating outside Japan. To help enhance collaboration between the private and public sectors in this area, Hitachi executives participated in the Council for Public-Private Cooperation for Overseas Safety organized by Japan's Ministry of Foreign Affairs, and in June 2014 Hitachi took part in a public-private kidnap incident preparatory training exercise.

* Incident in January 2013 in which an armed terrorist group attacked a natural gas refining plant in Algeria. There were more than 30 victims, including 10 Japanese.

Promoting Information Security

The Information Security Committee, chaired by the Chief Information Security Officer, determines our information security policies and procedures. The Information Security Promotion Council and other bodies convey decisions internally and to other companies in the Hitachi Group. Information security officers at business sites and companies ensure that these decisions are implemented in the workplace.

The Hitachi Group emphasizes two points in information security and personal information protection:

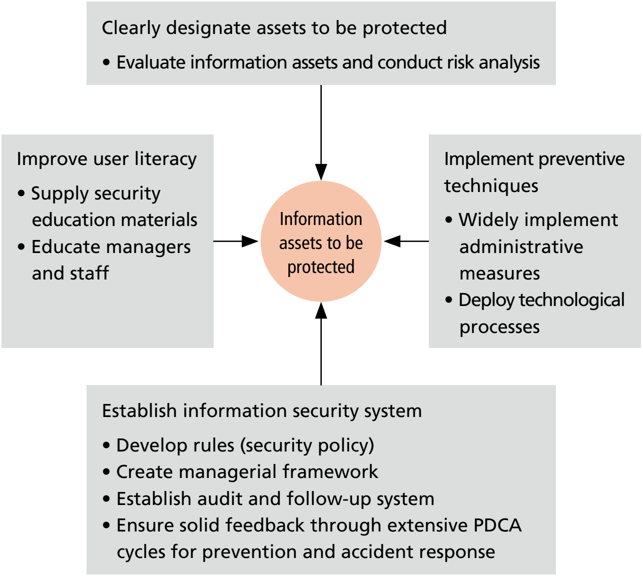
(1) Precautionary measures and prompt security responses

We classify assets to be secured and take safeguarding measures based on vulnerability and risk analyses. We also have an emergency manual for security breaches, based on the assumption that these are inevitable, and not just possible.

(2) Promoting stronger ethical and security awareness among data users

We have prepared a program tailored to Hitachi's various personnel levels and are working to raise the prevailing sense of ethics and security awareness through Group-wide e-learning. We are also conducting audits to identify and address problems early on.

Basic Approach to Information Security Governance



Clearly designate assets to be protected
- Evaluate information assets and conduct risk analysis

Improve user literacy
- Supply security education materials
- Educate managers and staff

Information assets to be protected

Implement preventive techniques
- Widely implement administrative measures
- Deploy technological processes

Establish information security system
- Develop rules (security policy)
- Create managerial framework
- Establish audit and follow-up system
- Ensure solid feedback through extensive PDCA cycles for prevention and accident response