Risk Management

Hitachi's Approach

Hitachi launched an Investment Strategy Committee in 2017 to ascertain and minimize risks and to strengthen the quantitative risk management of its investments. The Executive Sustainability Committee deliberates the social and environmental impact of our business activities to clarify any negative impact our business has on society and the environment and to identify countermeasures. We are reinforcing business continuity plans (BCPs) and further tightening our information security to ensure the stable supply of our products and services and to prevent threats to our networks that could severely disrupt business operations.

Our Impact on Society

No. of employees (Hitachi, Ltd.)

33,490

Our Performance

Recipients of e-learning programs on information security (Hitachi, Ltd.)

Approx. 40,000

Addressing Risks and Opportunities

Risks and Opportunities

Policy

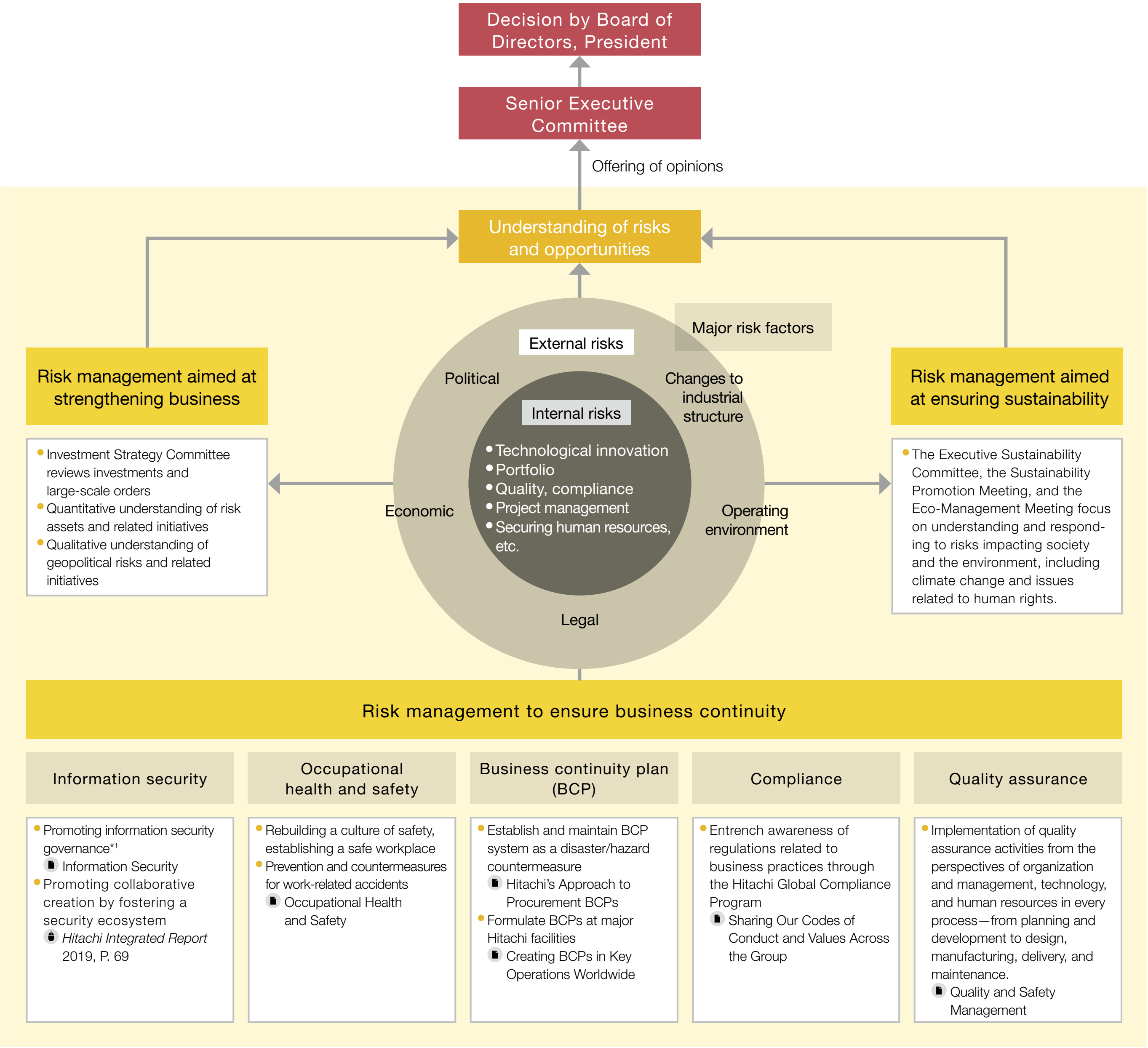
Hitachi's 2021 Mid-term Management Plan, beginning in fiscal 2019, focuses on expanding our business while making the best use of the Company's competitive advantages. In particular, we target investment for growth in select, focused areas over the three years through fiscal 2021 of ¥2.0–¥2.5 trillion, compared to investment of about ¥500 billion in the three years through fiscal 2018. We believe taking advantage of growth business opportunities and implementing aggressive management requires a solid risk management system.

Hitachi established the Investment Strategy Committee to strengthen investment risk management in 2017 and continues to work to better understand risk and take appropriate action. The Company in the same year established the Executive Sustainability Committee to focus on the company's policies in regard to social and environmental issues. Our efforts in this area also included a move to identify issues that could be seen as business opportunities, as well as the negative effects on society and the environment from our business activities and the measures Hitachi is taking to address them.

Risk Management System

Frameworks and Systems

The business environment is changing day by day, impacted by the continued advance of information and communications technology, as exemplified by IoT, and geopolitical risks arising from complex shifts in political and economic conditions around the world. Hitachi aims to create new revenue opportunities while controlling risk. To do this, we maintain a clear understanding and analysis of the operating environment, taking into account social issues as well as our competitive advantages and management resources, and conduct risk management with an eye toward the many risks the Company should be prepared for as well as opportunities for growth.



Decision by Board of Directors, President

Senior Executive Committee

Offering of opinions

Understanding of risks and opportunities

Major risk factors

External risks

Political

Changes to industrial structure

Economic

Operating environment

Legal

Internal risks

- Technological innovation
- Portfolio
- Quality, compliance
- Project management
- Securing human resources, etc.

Risk management aimed at strengthening business

- Investment Strategy Committee reviews investments and large-scale orders
- Quantitative understanding of risk assets and related initiatives
- Qualitative understanding of geopolitical risks and related initiatives

Risk management aimed at ensuring sustainability

- The Executive Sustainability Committee, the Sustainability Promotion Meeting, and the Eco-Management Meeting focus on understanding and responding to risks impacting society and the environment, including climate change and issues related to human rights.

Risk management to ensure business continuity

Information security

- Promoting information security governance[*1]
  - Information Security
- Promoting collaborative creation by fostering a security ecosystem
  - *Hitachi Integrated Report* 2019, P. 69

Occupational health and safety

- Rebuilding a culture of safety, establishing a safe workplace
- Prevention and countermeasures for work-related accidents
  - Occupational Health and Safety

Business continuity plan (BCP)

- Establish and maintain BCP system as a disaster/hazard countermeasure
  - Hitachi's Approach to Procurement BCPs
- Formulate BCPs at major Hitachi facilities
  - Creating BCPs in Key Operations Worldwide

Compliance

- Entrench awareness of regulations related to business practices through the Hitachi Global Compliance Program
  - Sharing Our Codes of Conduct and Values Across the Group

Quality assurance

- Implementation of quality assurance activities from the perspectives of organization and management, technology, and human resources in every process—from planning and development to design, manufacturing, delivery, and maintenance.
  - Quality and Safety Management

[*1] Information security governance works in support of corporate governance by building and maintaining an organization's internal control mechanisms related to information security.

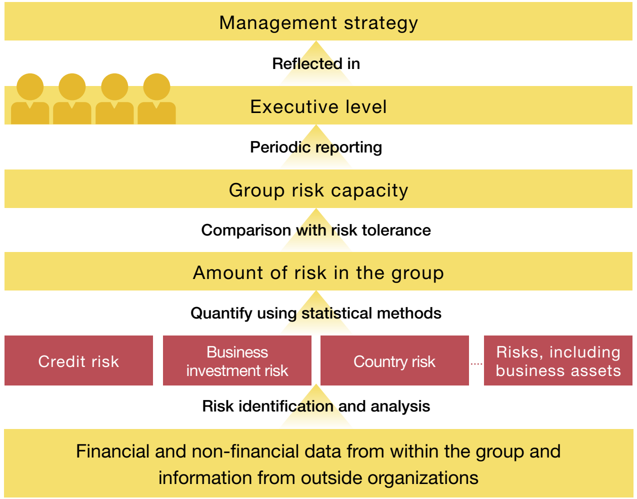
Understanding and Responding to Quantitative Risk

Frameworks and Systems

In regard to quantitative risk, assumed maximum risk (value at risk) is calculated using statistical methods based on the type of asset held. More specifically, value at risk measures the maximum expected loss based on price movements over a specified period of time (observation period) at a given confidence level for a defined period of time moving forward. Visualizing the strength of a company's balance sheet and whether that company has the potential for growth, including by focusing on whether the maximum expected loss is within the range of net assets or whether there is room to invest in growth, limits the likelihood that opportunities for growth will be missed, while continued monitoring ensures that risks do not exceed management capabilities.

Moreover, analyzing risk by country and sector, while also taking into account future trends, allows a quantitative understanding of the concentration of risks in a given country or sector relative to profitability.

The Flow of Quantitative Risk Assessment


Management strategy
Reflected in
Executive level
Periodic reporting
Group risk capacity
Comparison with risk tolerance
Amount of risk in the group
Quantify using statistical methods
Credit risk
Business investment risk
Country risk
Risks, including business assets
Risk identification and analysis
Financial and non-financial data from within the group and information from outside organizations

Understanding and Responding to Qualitative Risk

Objectives, Activities, and Achievements

In regard to qualitative risk, including geopolitical risk, we maintain a focus on the global political and economic situation by taking advantage of research from external organizations, and use this information to analyze the potential risks and opportunities for Hitachi so that we may take action to improve our corporate value. In addition, the Investment Strategy Committee examines investment projects and large orders, taking into account qualitative factors in addition to quantitative factors such as those listed below.

- Related technological innovations and competitive conditions
- Hitachi's past performance in the business
- Trends and market conditions, including prices and costs
- Business performance from ordering parties and their transaction history with Hitachi, etc.
- Contractual rights and obligations (transaction terms, reasons and details for damages and penalties)
- Local laws and labor practices in countries in which the business operates

Understanding and Responding to Risks and Opportunities Related to Sustainability

Objectives, Activities, and Achievements

Social and environmental issues, including climate change, resource depletion, the curtailment of business activity due to significant disasters, and social instability due to growing inequality, are having a substantial impact on corporate value creation and business models.

Amid such a drastic change in the business environment, companies must have a clear understanding of opportunities and risks and take appropriate measures if they are to achieve sustainable growth over the long term.

Hitachi is able to gain a clear understanding of sustainability-related risks, and accordingly take appropriate action, thanks to the efforts of the Executive Sustainability Committee and other related committees. We remain actively engaged in promoting our own sustainable growth while contributing to the realization of a sustainable society by seeking out business opportunities contributing to the resolution of important domestic and overseas issues, including those relevant to the UN Sustainable Development Goals (SDGs) and Society 5.0.

Risk Factors

Objectives, Activities, and Achievements

We conduct business on a global scale across a broad range of business areas and utilize sophisticated, specialized technologies to carry out our operations. Therefore, we are exposed to a wide range of risks related to our operations. The following risks are based on the assumptions we consider reasonable as of the date this report was issued.

For more information on business risks and other risks, please refer to our 150th *Annual Securities Report*.

Annual Securities Report

Major Risks and Opportunities

Major risk factors	Details on risks and opportunities		Company actions	
Fluctuations in product supply and demand, exchange rates and resource prices; insufficient raw materials, components	Risks	• Price fluctuations, including for products, exchange rate impact and excess inventory • Exchange rate impact and price fluctuations, including for raw materials and components • Impact from significant disasters on supply chain	• Building close relationships with multiple suppliers • Ensuring an appropriate response to changes in demand in each region by promoting a local production and local consumption model for products and services • Heightening resistance to business interruption risks by formulating BCPs at domestic and major overseas facilities	Responsible Procurement Stable Provision of Products and Services
Rapid technological innovation	Risks	• Decreased competitiveness if development of cutting-edge technology, or application to product/service does not progress as expected • Reduction or elimination of existing market due to technological innovation	• Promoting open innovation through industry-academia-government cooperation • Bolstering the digital workforce • Strengthen Lumada • Fostering an innovation ecosystem through the above	Research and Development (R&D) Developing Human Capital for Frontline and Digital Operations
	Opportunities	• Development of advanced technology leads to new business opportunities		
Securing human resources	Risks	• Impact on new hires and worker retention due to increased competition to hire and retain the highly skilled workers	• Securing the highly skilled global workers using a global common standard for personnel • Securing and training the highly skilled workers through in-house educational systems, include Hitachi Academy, and Hitachi University, the group's global common learning management system	2021 HR Strategy Developing Global Human Capital
	Opportunities	• Growth opportunities on the recruitment and retention of highly skilled workers that share the Hitachi vision		
Occupational health and safety	Risks	• Impact on business due to inability to create healthy, safe and secure work environments	• Establishing a global occupational health and safety system that includes lessons learned from global operations, entrenchment of global norms, and the sharing of success stories	Occupational Health and Safety
M&A, investment in new projects, etc.	Risks	• M&A aimed at strengthening the Social Innovation Business, investment in new projects, R&D investment/capex, failure related to insufficient project management in large-scale orders	• Implementing phase-gate management in each business unit (BU), analysis and discussion of market trends, strategies, acquisition prices, and the post-merger integration process at Investment Strategy Committee, Senior Executive Committee, Board of Directors, and Audit Committee	Independent Director Dialogue, *Hitachi Integrated Report 2019*, P. 18 Corporate Governance
	Opportunities	• Building a foundation for growth through the acquisition of new management resources		
Geopolitical risks	Risks	• Impact on Hitachi's overseas businesses due to global political, economic and social trends	• Regularly updating our understanding of global political and economic trends, analyzing the impact on our business, and swiftly implementing countermeasures on a groupwide basis	
Tighter laws and regulations	Risks	• Tighter laws and regulations in regard to investment, exports, and customs duties Example: The effects on business activities from the introduction of new laws and regulations related to the protection of personal data, such as the General Data Protection Regulation (GDPR) in Europe	• Operating of personal information protection systems in line with Hitachi's personal information protection policy • Identifying businesses subject to GDPR, assessing risk, implementing appropriate safety management measures in line with those risks, implementing worker training	Rigorous Information Management Information Security
Compliance	Risks	• Reduced trust and a decline in corporate value as a result of corporate behavior that deviates from social norms and violates laws, including relating to bribery and anti-competitive activities	• Implementing groupwide compliance programs and establishing the highest values in the Codes of Conduct • Strengthening measures to prevent bribery and violation of competition laws	Compliance
Product quality and responsibility	Risks	• Reduced trust and claims for damages due to defects or a deterioration in product and service quality as a result of the increased complexity/sophistication of products or services, or the diversification of production sites or suppliers	• Strengthening the quality assurance system • Activities aimed at preventing accidents • Activities aimed at ensuring compliance with laws and regulations related to technology • Intensive risk assessment • Implementing measures to handle product accidents • Conducting quality and reliability-related training	Quality and Safety Management
Climate change/significant disasters	Risks	• Impact on business activities due to measures in line with the tightening of international regulations to curb greenhouse gas emissions and the depletion of energy and resources • Impact on business activities, from production to sales, due to significant disaster affecting major Hitachi facilities in Japan or overseas	• Strengthening measures aimed at achieving the CO_2 reduction targets in the Hitachi Environmental Innovation 2050 • Enacting measures in line with an analysis of Hitachi risks and opportunities based on climate-related scenarios • Formulating BCPs to strengthen our ability to respond to business disruption risks	Achieving a Low-Carbon Society Climate-related Information Disclosure (Based on TCFD Recommendations) Stable Provision of Products and Services
	Opportunities	• Expansion in the decarbonization business through offering climate-change-related solutions		
Information security	Risks	• Computer viruses or other factors adversely impacting information systems	• Promoting cybersecurity strategies through risk management and value creation	Information Security Story of Value Creation in the IT Sector, *Hitachi Integrated Report 2019*, P. 54
	Opportunities	• Expansion in revenue opportunities through increased demand for information security measures		

Stable Provision of Products and Services

Hitachi's Thinking on BCPs

Policy

Given the close relation of our business to social infrastructure, we are enhancing our business continuity plans (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 (Overview)* in Japanese. In fiscal 2010 this was translated into English and Chinese for distribution to all Hitachi Group companies worldwide to ensure our response readiness for large disasters and other risks.

Creating BCPs in Key Operations Worldwide

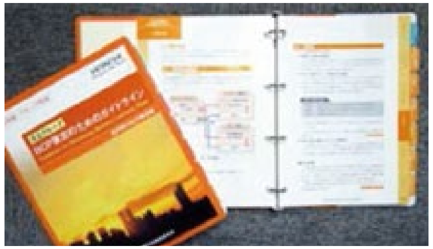
Frameworks and Systems

When the Great East Japan Earthquake struck in March 2011, quick responses and swift decision making were enabled by the BCPs that we had developed based on the *Hitachi Group Guidelines for Developing Business Continuity Plans (Overview)*. 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 versions of the *Hitachi Group Guidelines for Developing Business Continuity Plans (By Department)* to further improve our BCPs.

By the end of fiscal 2011, Hitachi Group operations in Japan had completed their preparation and review of BCPs for both large earthquakes and novel strains of influenza as appropriate to their operations.

On top of these efforts, Hitachi, Ltd. has held annual earth-quake drills simulating a major seismic event at key operations in Japan since fiscal 1998. In March 2018, we held initial response drills at our headquarters under the direction of our head of Major Earthquake Countermeasures Office simulating a large earthquake in the suburbs of Tokyo, striving to promote understanding of each department's role and strengthen cooperation among departments. As part of countermeasures against large earthquakes striking the suburbs of Tokyo, in December 2017 we developed action plans including setting up substitute headquarters in the Kansai region in case our Tokyo headquarters cease to function temporarily due to such earthquakes. In March 2019, based on the scenario of an earthquake striking the Tokyo metropolitan area and significantly damaging its infrastructure, we established a substitute headquarters at our Kansai Area Operation and conducted initial response drills and joint drills with the response headquarters at our Tokyo headquarters according to our action plans.

Hitachi appointed personnel with responsibility for risk-response policies at its main overseas bases in fiscal 2013. By the end of that year, around 300 companies prepared BCPs with the goal of completing them for key operations. 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.



Hitachi Group Guidelines for Developing Business Continuity Plans (By Department).

Earthquake simulation drill.

Hitachi's Approach to Procurement BCPs

Policy

We have a deep involvement in social infrastructures in places where the suppliers who are our business partners can be affected by major earthquakes and other natural disasters.

These disasters can heavily impact not only our business operations and those of our suppliers but also society as a whole. To minimize this impact, the procurement divisions in business units and key Group companies in Japan have created procurement BCPs that (1) standardize and use generic parts to make procurement as flexible as possible; (2) cultivate multiple suppliers;

(3) distribute production across several locations; (4) budget inventory strategically; and (5) consider substitute products.

Creation of Procurement BCPs

Frameworks and Systems

To see whether or not procurement BCPs would be effective, we held desktop exercises to discuss in a group what should be done during and after a disaster, making further improvements as a result.

In fiscal 2018, all major Group business sites with production lines (approximately 210 sites in total) took steps to maintain and strengthen the procurement BCPs they had created by the previous fiscal year, thereby contributing to the continuation of Hitachi's global operations.

Improving Safety for Employees Sent to Dangerous Regions

Frameworks and Systems

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 to countries and areas at higher risk. 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 2018, against the threat of terrorism expanding around the world and infectious diseases spreading regionally, we had in place a range of safety measures, including providing timely alerts to employees. This underscores 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. Since 2014 Hitachi has taken part in public-private kidnap incident preparatory training exercises.

Information Security

Information Security Policies

Policy

The increased connections between things due to development of IoT are creating new value. At the same time, increasingly sophisticated cyberattacks are widening their focus from traditional IT to include the IoT/OT field. Managing information security risks is one of the most critical issues for companies to minimize the risk of business disruption due to factors such as leaks of information or operational stoppages.

The development of the Social Innovation Business has highlighted for Hitachi the vital importance of information security governance as a key management issue. The Japan Business Federation's Declaration of Cyber Security Management that was published in March 2018 also placed emphasis on cyber security measures as a critical management challenge from the aspects of both value creation and risk management. Hitachi approaches the issue of information security governance based on the same concept.

At the same time, as a global company, we regard cyber security risk as one of our management risks. Accordingly, to allow us to declare both internally and externally Group policies for addressing this risk, we have formulated Information Security Policies in line with our corporate management policies and based on our cyber security risk management.

Information Security Policies

1. Formulation and continuous improvement to information security management regulations
2. Protection and continuous management of information assets
3. Strict observance of laws and standards
4. Education and training
5. Incident prevention and management
6. Assurance of fair business practices within the corporate group

Three Principles for Preventing Leakage of Confidential Information

Policy

Hitachi, Ltd. has formulated the Three Principles for Preventing Leakage of Confidential Information to ensure the highest level of care for such information and to prevent leaks and other related incidents. Our policies specify that if an incident does occur, damage must be promptly minimized by contacting customers, reporting to government agencies, investigating causes, and acting to prevent any recurrence.

Three Principles for Preventing Leakage of Confidential Information

Principle 1: In principle, no confidential information shall be taken outside of the company's premises.

Principle 2: Any person taking confidential information out of the company's premises when necessary for conducting business shall obtain prior approval from the Information Asset Manager.

Principle 3: Any person taking confidential information out of the company's premises when necessary for conducting business shall carry out the necessary and appropriate measures to prevent information leakage.

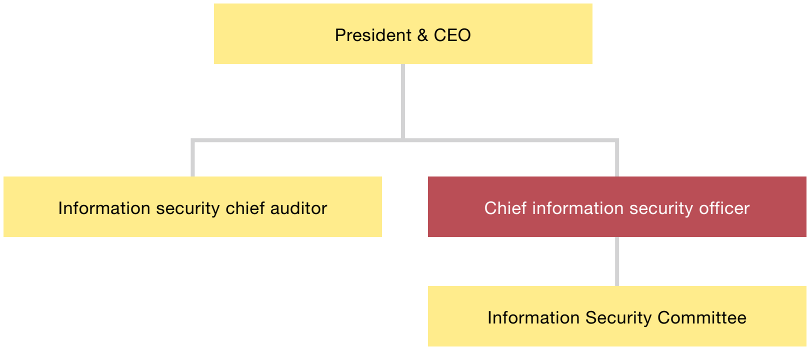
Framework for Promoting Information Security

Frameworks and Systems

At Hitachi, Ltd. the senior executive with ultimate authority and responsibility regarding the handling of information security and personal privacy issues is appointed by the president and CEO. Hitachi established a position of chief information security officer (CISO) to oversee promotion of information security for all Hitachi products and internal facilities. In fiscal 2018, the CISO role was performed by an executive vice president.

Chaired by the CISO, the Information Security Committee determines all policies and procedures for information security and personal information protection. These decisions are conveyed to all Hitachi Group business sites and companies, and are implemented by the relevant information security officers.

Framework for Promoting Information Security


President & CEO
Information security chief auditor
Chief information security officer
Information Security Committee

Information Security Management

Frameworks and Systems

Hitachi Group companies worldwide reinforce their information security in line with our Global Information Security Administration Rules, which conform to the international ISO/IEC 27001 standard. These rules are globally distributed from the parent company in Japan to Group companies worldwide. Other measures include the provision of shared security services and related support for information security by the regional headquarters in the Americas, Europe, Southeast Asia, China, and India.

Security Monitoring

In Hitachi, the Security Operation Center (SOC) monitors security on a 24/7 basis so cyberattacks can be detected and countermeasures initiated right away. The Incident Response Team (IRT) collects and develops threat intelligence*[1] and manages the response to any security incidents.

*[1] Threat intelligence: An approach to countering cyber attacks using knowledge of new threats gathered from a range of information on cyber security.

Implementing Rigorous Information Security

Frameworks and Systems

The Information Security Committee determines policies and procedures for information security and personal information protection. 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 clarify the principal systems and assets to be secured, using vulnerability and risk analyses to formulate companywide business continuity plans (BCPs) for cyber incidents and to implement safeguarding measures. We also have an emergency process manual for security breaches, based on the assumption that these are inevitable, and not just possible.

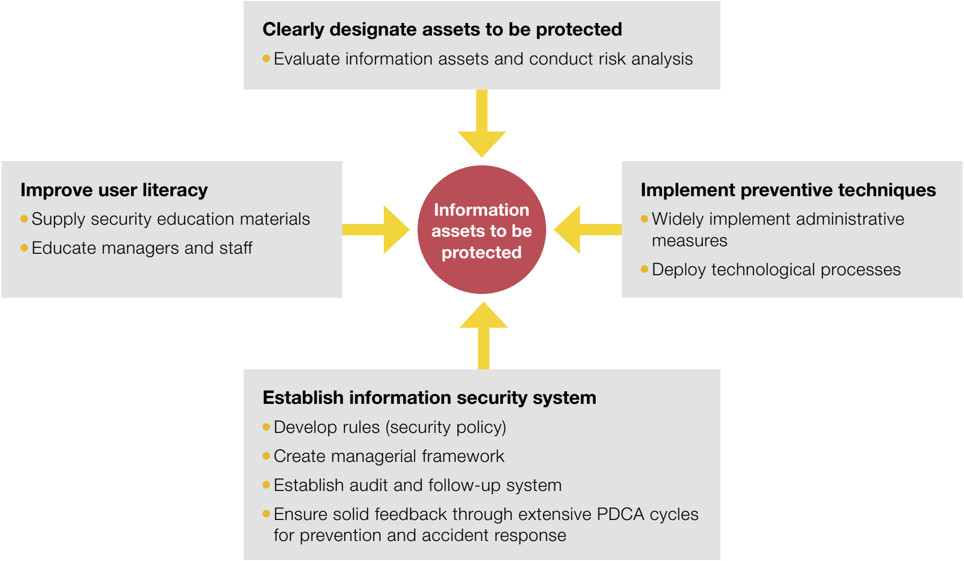
(2) Promoting stronger ethical and security awareness among data users

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.

Details, including a message from the CISO and a list of third-party assessments and certifications, are contained in Information Security Report 2018.

Information Security Report 2018

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

Preventing Information Leaks

Frameworks and Systems

Hitachi takes the following IT steps to prevent information leaks: encrypting devices; using thin clients;*[1] employing electronic document access control and expiration processing software; maintaining ID management and access control by building an authentication infrastructure; and filtering e-mail and visited websites. In response to the recent spate of targeted e-mail attacks and other cyberattacks, we are participating in an initiative to share information between the private sector and the government. We are also enhancing our IT organization by adding more layers to our leak prevention procedures.

To ensure the secure exchange of information with our suppliers, we review their information security measures based on Hitachi's own standards before allowing them access to confidential information. We have provided tools to suppliers (procurement partners) for security education and for checking business information on computers. In addition, we require suppliers to check and remove business information from personal computers to prevent leaks.

*1 Thin client: A terminal with the minimum necessary software. Thin client computing significantly enhances cyber security by storing applications and data on the server.

Education on Information Security

Objectives, Activities, and Achievements

Consistently maintaining information security requires all employees to continually develop their knowledge of information handling and to remain strongly aware of the issues. For this reason, we hold annual e-learning programs on information security and personal information protection for all directors, employees, and temporary employees.

Nearly all of the roughly 40,000 employees at Hitachi, Ltd. participate in these programs. We offer a variety of courses that have different goals and are tailored to different target audiences, including new employees, new managers, and information system administrators. In 2012, we also began simulation training to educate employees about malicious targeted e-mail attacks and other cyberattacks. Employees are sent examples of targeted e-mail to heighten their awareness of security through direct experience.

Our educational programs, available to Hitachi Group companies in Japan and other global regions, provide Group-wide education on information security and personal information protection.

Thorough Information Security Audits and Inspections ✓

Objectives, Activities, and Achievements

The Hitachi Group has developed its approach to security based on the "plan-do-check-act" (PDCA) cycle for its information security management system. We conduct annual information security and personal information protection audits at all Group companies and business units.

The president of Hitachi, Ltd. appoints officers to conduct independent audits. These officers are not allowed to audit their own units, underlining our commitment to fairness and objectivity in auditing. There are 220 Hitachi Group companies in Japan, including Hitachi, Ltd., that conduct audits in the same way as Hitachi, Ltd., and all results are subject to confirmation. For Hitachi Group companies outside Japan, we use a "common global self-check" approach to ensure Group-wide auditing and inspections. We implement Confirmation of Personal Information Protection and Information Security Management annually for the voluntary inspection of Hitachi, Ltd. business unit workplaces. We conduct monthly Confirmation of Personal Information Protection and Information Security Management assessments at 606 operations (as of March 2019) that handle important personal information. This regular control mechanism ensures ample safety management and implementation.