Disaster Risk Management

Crisis Management and Business Continuity Plan

Responses to risks such as natural disasters, pandemics, serious accidents/incidents

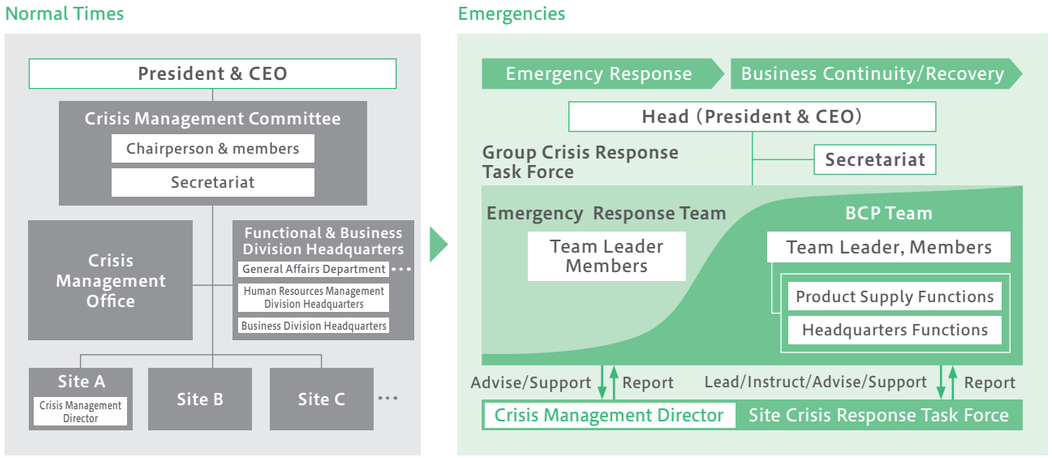
NSK's Approach

NSK's basic policy is to protect business infrastructures, including securing human lives as a top priority and to resume business activities as soon as possible in the event of crisis. On that basis, we are working to formulate and improve a Business Continuity Plan (BCP) to prevent crises from occurring as well as to minimize damage and shorten the recovery period if a crisis is materialized.

Disaster Risk Management System

By establishing and improving crisis management systems to prepare for relevant risks, primarily natural disasters, pandemics, and serious accidents/incidents, etc., the Crisis Management Committee aims to minimize the damage in the event of an actual emergency, while playing a role in addressing such situations swiftly and effectively. Such organizations have also been established in each region outside Japan to supervise crisis management in their respective locations. When a relevant emergency occurs, the Crisis Management Committee in Japan works with the organizations concerned to deal with the crisis.

■ Crisis Management Structure



Examples of FY2021 Initiatives

Checking BCM/BCP Systems Based on Check Sheets

Concerning our Business Continuity Management (BCM) system, which was rebuilt following the Great East Japan Earthquake, we prepared a self evaluation sheet to ascertain the Company's level of preparedness and to check for any omissions, conducted inspections of headquarters functions in all regions, and identified any issues.

We also carried out a review of our BCP guidelines, inspected the implementation status of measures based on the check sheets at each business site, and clarified any areas in need of improvement.

Workshops Based on Specific Disaster Scenarios

To strengthen the capabilities of the Group Crisis Response Task Force, with the participation of relevant departments we held three workshops. Based on specific disaster scenarios, we identified emergency actions and the tasks needed to put them into effect.

More than 50 people attended each workshop. By holding group discussions on the propositions made in online conferences and sharing the results, this led to the identification of issues in preparation for an online conference of the Group Crisis Response Task Force.

▸ **Please see our website for more information.** https://www.nsk.com/sustainability/disasterRiskmanagement/index.html

Information Security Management

NSK's Approach

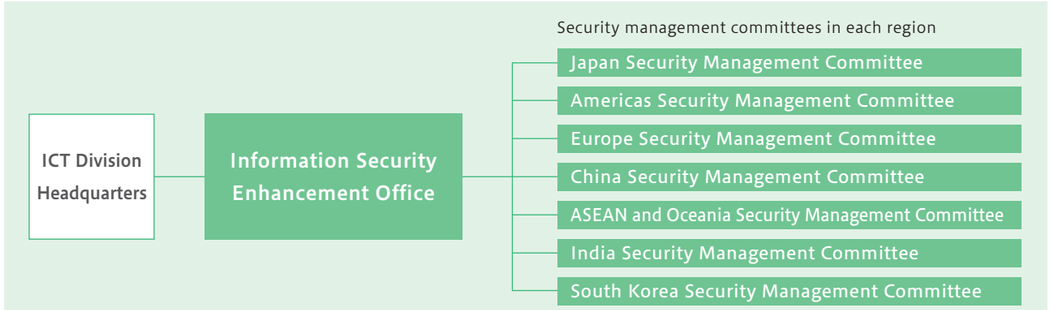
Recent advances in information and communications technology (ICT) have dramatically enhanced the convenience of information handling. However, in addition to the risk of mishandling information, there is a greater risk of information being stolen or leaked through sophisticated cyberattacks or due to the growing number of people working from home. Positioning information security management as one of its important management tasks, NSK is working to reduce risk and strengthen its response to relevant laws and regulations.

Moreover, we are promoting initiatives for more robust mechanisms and organizational structures, such as network countermeasures, against increasingly sophisticated cyberattacks.

Information Security System

The NSK Group established the Information Security Enhancement Office under the ICT Division HQ to implement more comprehensive information security enhancement measures globally. Moreover, regarding information security–related risks, in connection with the Corporate Risk Management System, the Board of Directors discusses issues related to information security measures and oversees risk mitigation for the entire Group. The Information Security Enhancement Office regularly holds global meetings, and plans and implements information security measures for the Group, working in cooperation with information security management committees in Japan, the Americas, Europe, China, ASEAN and Oceania, India, and South Korea.

■ Information Security Management System



Examples of FY2021 Initiatives

Status of System Preparations for Retaining ISO27001 Certification

The Company will continue efforts to retain ISO27001 certification at previously certified sites (Japan, South Korea, India).

In addition, based on demands from customers, in FY2021 the Company acquired TISAX, a security certification broadly adopted in Germany's automobile industry, at two new sites. Moreover, the Company is working to acquire this certification for three sites in China and two new sites in Europe.

Cyberattack Countermeasures and Training

As in the previous year, the Company provided targeted threat e-mail training to all NSK Group employees, including those at overseas sites, and conducted training that assumes the occurrence of incidents in cooperation with the Systems Management Department. Some of the technological measures the Company has promoted from the viewpoint of preventing damages from recent ransomware attacks include VPN device vulnerability assessments and countermeasures, as well as phishing e-mail monitoring enhancement countermeasures.

Moreover, given the growing risk of attacks against the supply chain, the Company enhanced security systems at its factories and implemented asset identification and risk assessments for control equipment.

▸ **Please see our website for more information.** https://www.nsk.com/sustainability/infoSecurity/index.html