Business Continuity Management

Nomura Group regards natural disasters such as earthquakes and typhoons, manmade disasters such as fires and terrorism, infectious diseases like coronavirus, system failures, and information asset leaks as the key types of crises that must be prepared for. In the event for such crisis, we have established a global business continuity framework and work on a wide range of measures, including educating our people about our disaster response measures.

Business continuity framework

The Group Crisis Management Committee is tasked with preparing for crises, and under the committee's leadership the Group has been continually strengthening the crisis management program and the business continuity framework both in Japan and overseas. The Group Crisis Management Committee is chaired by a senior officer appointed by the Group CEO, and comprises senior officers from Group companies. Resolutions passed by the committee are reported to the Executive Management Board. In the event of a major disaster, the committee establishes a command center and takes appropriate measures to confirm the safety of employees and their families, ensure safety, prevent the spread of damage, and maintain business continuity arrangements.

As a specific example of this business continuity framework, in the event that key offices are rendered unusable due to an earthquake, a typhoon, or any other natural disaster caused by climate change, we are prepared to respond remotely in addition to continuing operations at the backup office. We also have a remote backup data center that protects critical data and applications in the event of a data center failure. Furthermore, we have bolstered our infrastructure, which includes power generators, so that in the event of a power down affecting a wide area, such as a powerful earthquake directly beneath the Tokyo metropolitan area, we can continue our critical functions to avoid systemic risk and to protect our clients from being impacted. Similar infrastructure have also been put in place at our key overseas offices.

In response to the coronavirus pandemic, and in accordance with our Group guidelines and requests from the national and local governments, we have implemented measures to prevent the spread of infections and to secure a system for business continuity by keeping employees from entering the office through telecommuting and rotations, restricting travel on business trips, and refraining from activities that may contribute to infection, such as holding seminars and meetings. At our key overseas offices, we have ensured business continuity through remote work.

In Japan, the Crisis Management Committee Office regularly conducts employee safety confirmation drills, disaster prevention drills, and business continuity drills to ensure that we are able to respond quickly should a crisis occur. At overseas offices, these exercises are carried out by the Business Continuity Management Team in each location. Through these and other efforts, we aim to become more proficient at handling crises and strengthen our systems for managing them.

Business continuity initiatives

1 Strengthen the business continuity framework

Maintain/enhance backup offices / Secure emergency response personnel / Maintain/enhance emergency communication equipment / Enhance telework environment

2 Periodic drills and training

Employee safety confirmation drills / Drills based on business continuity plan (BCP) / Initial response training and drills simulating earthquake with epicenter directly under Tokyo or other massive earthquake / Nankai Trough earthquake response training at branch offices

3 Strengthen collaboration between Group companies in Japan and overseas

Enhance information-sharing with Group companies in Japan / Enhance information-sharing framework with overseas Group companies

4 Business Continuity Plan

Review and revise the Business Continuity Plan for the scenarios of a massive natural disaster or a massive system failure

Cyber Security

Business Continuity Management

In order to ensure that clients' information and assets are securely protected from increasingly challenging cyber security threats, and to enable clients to conduct transactions with peace of mind, Nomura Group is working to strengthen its cyber security platform under the leadership of the Crisis Management Committee and Group Information Security Officer, using the Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc. of the Financial Services Agency, the Cybersecurity Framework of the National Institute of Standards and Technology (NIST) and other overseas frameworks, as references.

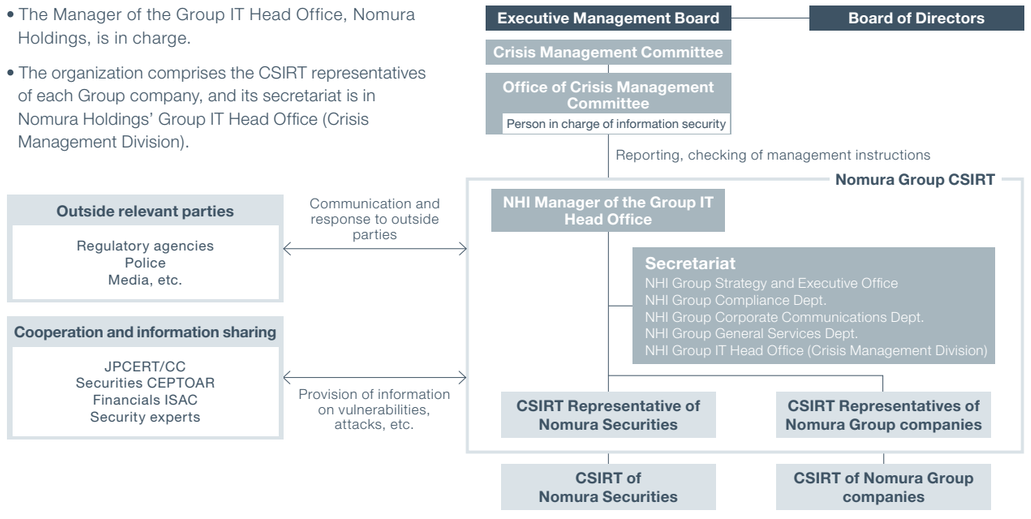
Recently, we have been promoting a review of the governance system in light of the progress in the use of cloud services as one of the key points to strengthen. We will continue to respond promptly to changes in the situation in close cooperation with other financial institutions, security specialists, and government agencies.

Cyber security system

Nomura Group has established the Nomura Group Computer Security Incident Response Team (CSIRT) under the Crisis Management Committee's secretariat, and has established a global structure for responding to incidents stemming from cyber-attacks and mitigating damage. In addition, Nomura Securities and Nomura Group companies have established CSIRTs to protect their operations, information assets, and systems

Organizational structure

- The Manager of the Group IT Head Office, Nomura Holdings, is in charge.
- The organization comprises the CSIRT representatives of each Group company, and its secretariat is in Nomura Holdings' Group IT Head Office (Crisis Management Division).



Organization management	At normal times, we take part in cyber security drills, conduct Threat-Led Penetration Test, assess cyber risks and monitor actions taken by overseas subsidiaries and outside contractors in a constant effort to heighten our readiness. In the case of an incident such as obtaining dangerous vulnerability information or detecting a cyber-attack, the CSIRT leads the efforts to analyze the cause, minimize damage, and quickly restore systems.
System security measures	We adopt a multi-layered defense system, which includes multiple detection and defense mechanisms against unauthorized access and malicious programs such as computer viruses. We review these countermeasures as appropriate to deal with new threats.
Human-level response	In accordance with the Nomura Group Information Security Policy, relevant seminars and training programs are regularly provided to all executives and employees and they are kept alert in order to raise their awareness and knowledge about cyber security.
Cooperation with outside organizations	Nomura is cooperating with information sharing organizations such as Financial ISAC Japan and FS-ISAC and cyber security vendors to gather and share information on the cyber attackers and their approaches.