BUSINESS CONTINUITY MANAGEMENT

Nomura Group regards natural disasters such as earthquakes and typhoons, man-made 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 a 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 functions as the Command Center to lead the Group’s response.

As a specific example of this business continuity framework, a system has been enforced so that operations can be continued at backup offices in the event that key offices are rendered unusable due to an earthquake or other disaster. 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 failure, we can continue our operations.

In response to the coronavirus pandemic, and in accordance with Group guidelines, we worked to prevent the spread of the virus before significant outbreaks occurred in Japan and overseas by restricting travel and other activities that could accelerate its spread. When the Japanese government declared a state of emergency we temporarily suspended business operations at domestic branches. We have also enhanced the remote work capability and established a work system that has allowed us to both continue our business operations and prevent the spread of coronavirus. 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.

CYBER SECURITY

Nomura Group has for some time been undertaking security measures to protect systems against cyber-attacks. However, in light of the increasingly serious cyber security threats throughout the world, we recognize that our current countermeasures may not be sufficient in the future. In addition, in the financial sector, digitalization is proceeding at an accelerating pace. The connection of all financial systems to networks may increase the cyber security risk. In order to ensure that clients’ information and assets are securely protected from these 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, using the Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc. of the Financial Services Agency, and the Cybersecurity Management Guidelines of the Ministry of Economy, Trade and Industry based on ISO27001 and ISO27002, as references.

Cyber security system

Nomura Group, as a whole, has established a global organizational structure to deal with incidents stemming from cyber-attacks and to minimize potential damage. The Nomura Group Computer Security Incident Response Team (CSIRT), formed within Nomura Holdings, has spearheaded the formation of a CSIRT in Nomura Securities and other Group companies, and governs the CSIRT in each Group company. Each CSIRT works to protect its company’s operational and information assets, as well as systems, promoting cyber security measures from four vantagepoints: organizational management, system security measures, human-level response, and coordination with outside organizations.

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 (Cybersecurity Management Division).
- The CSIRT leads the efforts to analyze the cause, minimize damage, and quickly restore systems.
- At normal times, we take part in cyber security drills, conduct Threat-Led Penetration Test, assess cyber risks and monitor actions taken by overseas authorities and outside contractors to boost 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 rapidly restore systems.
- Nomura is cooperating with information sharing organizations such as Financial ISAC Japan and FSA-ISAC and cyber security vendors to gather and share information on the cyber attackers and their approaches.