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 down affecting a wide area, such as a powerful earthquake directly beneath the Tokyo metropolitan area, we can continue our services. Nomura Group regards natural disasters from four vantage points: organizational management, system security measures, human-level response, and coordination with outside organizations.

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

Business continuity initiatives

1. Strengthen the business continuity framework
   - Maintain/Enhance backup offices / Secure emergency response personnel
   - Maintain/Enhance emergency communication equipment / Enhance network 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