Business Continuity Management

In Nomura Group, natural disasters such as earthquakes and typhoons, man-made disasters such as fires and terrorism, infectious diseases such as the COVID-19, system failures, and information asset leaks are considered as crisis events that must be prepared for. In order to respond to such an event, we have a comprehensive global business continuity framework and are working on a broad range of measures, including awareness raising activities for our employees.

Nomura Group has organized the Group Crisis Management Committee to continually strengthen the capability of the business continuity in Japan as well as outside of Japan. The Group Crisis Management Committee is chaired by a senior officer appointed by the Group CEO, and comprised of senior management 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 ensure the safety of employees and their families, control the spread of damage, and maintain business continuity arrangements.

Business continuity initiatives

1 Strengthen the business continuity framework

Maintain backup offices / Secure emergency response personnel / Maintain emergency communication equipment / Enhance remote work capability

2 Periodic drills and training

Employee safety confirmation drills / Drills based on Business Continuity Plan (BCP) / Response training based on Tokyo metropolitan earthquake scenario / Nankai Trough earthquake training

3 Strengthen collaboration between Group companies in Japan and overseas

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

4 Business Continuity Plan

Review and update the Business Continuity Plan based on wide area disasters such as earthquake in metropolitan area and large scale system failure

PDCA cycle for business continuity in normal times

Plan
Formulate policies / Design strategies

Do
Build framework / Analyze impact on business / Establish and update Business Continuity Plan / Drills

Check
Evaluate

Action
Maintain and improve

Responses in an emergency

Disaster occurs → Assess → Respond → Recover

Safety confirmation
Status of employees and their families

Status assessment
Damage to buildings and systems

BCP activation
Establish command center, activate backup office and remote working

Recovery
Ascertain the number of employees who can return to office, restore infrastructure, etc.

Cybersecurity

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 continues to strengthen its cyber security platform under the leadership of the Crisis Management Committee and Group IT Officer.

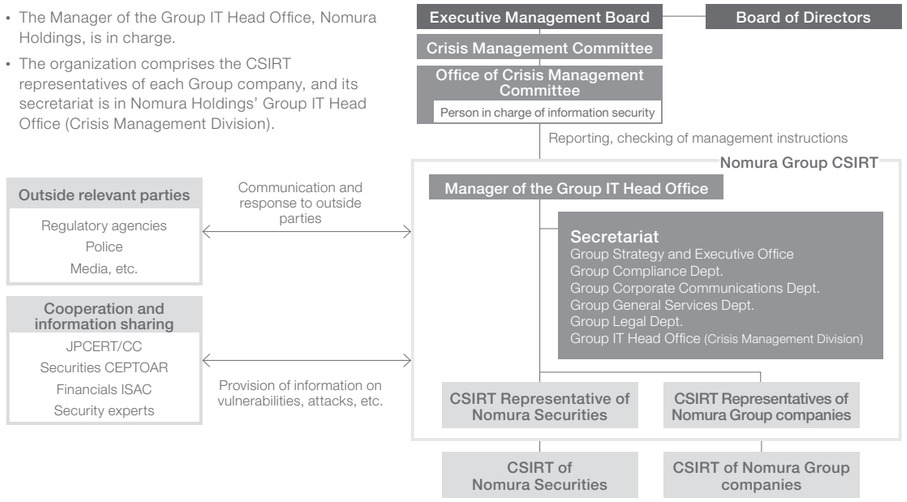
The leadership team will be leveraging the Comprehensive Guidelines for Supervision of Financial Instruments Business Operators, etc. of the Financial Services Agency, the Cybersecurity Framework of the National Institute of Standards and Technology (NIST) and other overseas frameworks, as references to manage the Cybersecurity operations throughout the entire Nomura Group.

Nomura Group has established the Nomura Group Computer Security Incident Response Team (CSIRT) under the Crisis Management Committee's secretariat.

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).



Cyber countermeasures

The following cyber countermeasures are being promoted for each of the five functional categories defined by the NIST Cybersecurity Framework.

Identify

- Based on our management vision and risk appetite, we have identified information assets to be protected, and have established a Group-wide governance system.
- We are continuously strengthening our system through threat-based penetration testing and third-party risk assessments.
- We are conducting cyber risk assessments and countermeasures, including programs utilizing support from outside vendors.

Protect

- We have deployed several system-related measures to protect against unauthorized access and computer viruses.
- We regularly implement training, drills, and awareness-raising activities to increase the knowledge of executives and employees.
- We have established a system to collect and share information on attackers and attack methods through communication with Financials ISAC Japan and specialized cyber security vendors.

Detect

- We have established a monitoring system that operates 24 hours a day, 365 days a year, to detect abnormalities in a timely manner.
- We have created a mechanism to collect and analyze system logs and to detect abnormalities, including internal misconduct.

Respond

- In preparation for cyber incidents, we have established a system for quickly contacting clients, related institutions, and senior management.
- We have created an incident response manual, and we analyze the cause of incidents, minimize damage, and otherwise respond mainly through CSIRT.

Recover

- We have established a business continuity plan and a backup data center.
- We have prepared for rapid recovery of business and systems through system switching training and cyber exercises.