

Risk Management

Fundamental Approach

Nomura Group has established processes to accurately identify risks arising from all types of operations and trading, and is working to bolster risk evaluation and the risk management framework.

Risk management policy

Our business activities are exposed to various risks including market risk, credit risk, operational risk, and liquidity risk. Properly managing these risks is one of management's top priorities.

In order to maintain capital adequacy and achieve its business plans under any type of economic environment, Nomura Group has defined the types and maximum levels of risk that the firm is willing to take, as documented in the Risk Appetite Statement.

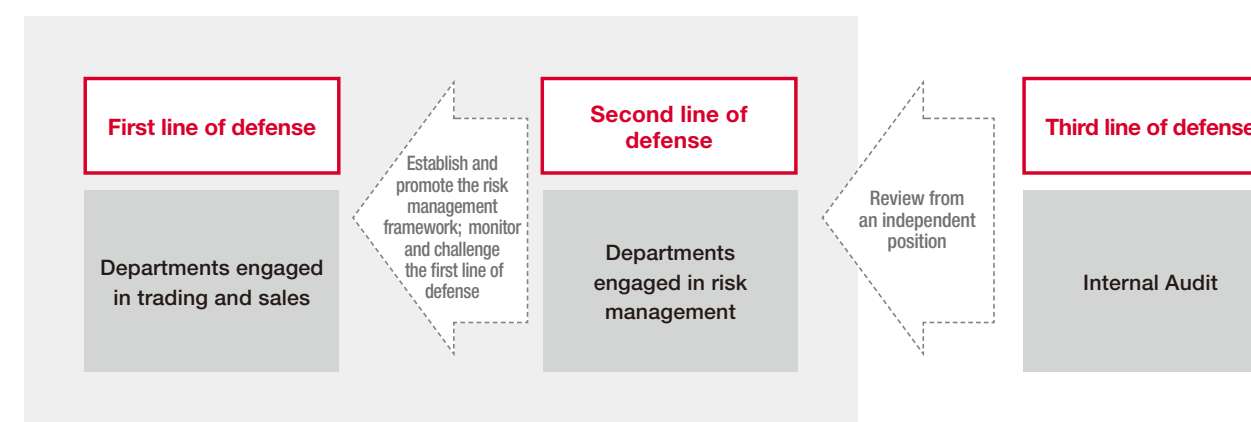
Risk culture

Fostering a sound risk culture is essential for Nomura Group to maintain its social credibility and sustain its business activities.

At Nomura Group, all employees, irrespective of their function or geographic location, must understand their specific responsibilities related to risk management, and actively work to manage risks. We aim to embed this risk culture throughout the firm through various training courses, as well as company rules and regulations.

The three lines of defense in risk management

Nomura Group has adopted the following layered structure on the grounds that all employees are accountable for proactively managing risk.



First line of defense	Second line of defense	Third line of defense
Departments engaged in trading and sales	Departments engaged in risk management	Internal Audit
<p>As the first line of defense, departments engaged in sales and trading manage the risks associated with their own business activities.</p> <p>For example, trading departments do business within predetermined risk limits, and proactively identify and address any issues they find.</p>	<p>Departments engaged in risk management establish frameworks to manage each type of risk, and support risk management measures taken by sales and trading departments, which are the First Line of Defense.</p> <p>Risk management departments independently monitor risks, and keep trading and sales departments in check as needed.</p>	<p>Internal Audit reviews and provides consulting from an independent, objective position, with the aim of adding value by improving the organization's operations and frameworks, including risk management.</p>

Risk management framework

Nomura Group has established a risk management framework based on risk profiles, as shown in the table below. We have also adopted a multi-faceted risk evaluation process to avoid risks that may be damaging to our reputation.

Risk management oversight is carried out by the

committees comprising members of senior management. The Group Integrated Risk Management Committee (GIRMC) and Global Risk Management Committee (GRMC), for example, deliberate and decide on risk management issues material to the firm.

Key Risk Types	Description	Related Divisions		
		Retail	Asset Management	Wholesale
Market risk	Risk of losses arising from fluctuations in values of financial assets and debt (including off balance sheet items) due to fluctuations in market risk factors (including interest rates, foreign exchange rates, and securities prices)		○	○
Credit risk	Risk of losses arising from the inability of an obligor or counterparty to fulfill their obligations under the terms of a previously agreed contract as the result of default, bankruptcy, or legal proceedings	○		○
Operational risk	Risk of losses arising from inadequate or failed internal processes, people, and systems or from external events	○	○	○
Liquidity risk	Risk of losses arising from a potential lack of access to funds or higher cost of funding than normal levels due to a deterioration in Nomura's creditworthiness or deterioration in market conditions			○

Adapting to the globalization of risk

We have observed the impact of the financial crisis in Europe and the US on the world economy. We have also witnessed economic developments in Asia influencing global energy prices. In terms of risk management, we must increasingly address risk on a global level.

Nomura Group has Risk Management Departments in five regions and seven countries. In addition to managing risks particular to their individual region, these Risk Management Departments work in close cooperation across the globe to ascertain and lessen the impact that risks may have on other regions.



Stress testing

Nomura Group conducts stress testing to address risks that may spread globally, and to identify risks that are difficult to recognize with statistical methods alone, as well as to prepare for unprecedented risk events.

Stress testing uses stress scenarios to assess the impact on our business and financial soundness should those adverse events occur. These scenarios may include severe deterioration in the economic environment, geopolitical conflicts, and natural disasters.

Examples of stress scenarios



Assessment of capital adequacy under the scenario that a serious economic situation that occurred in the past happens again (Example: Financial crisis)



Assessment of the impact on Nomura's earnings of extreme economic conditions that could occur in the future (Example: Economic collapse in a particular country or region)



Assessment of the impact on Nomura's portfolio of political events in Japan or overseas (Example: UK referendum on leaving EU)

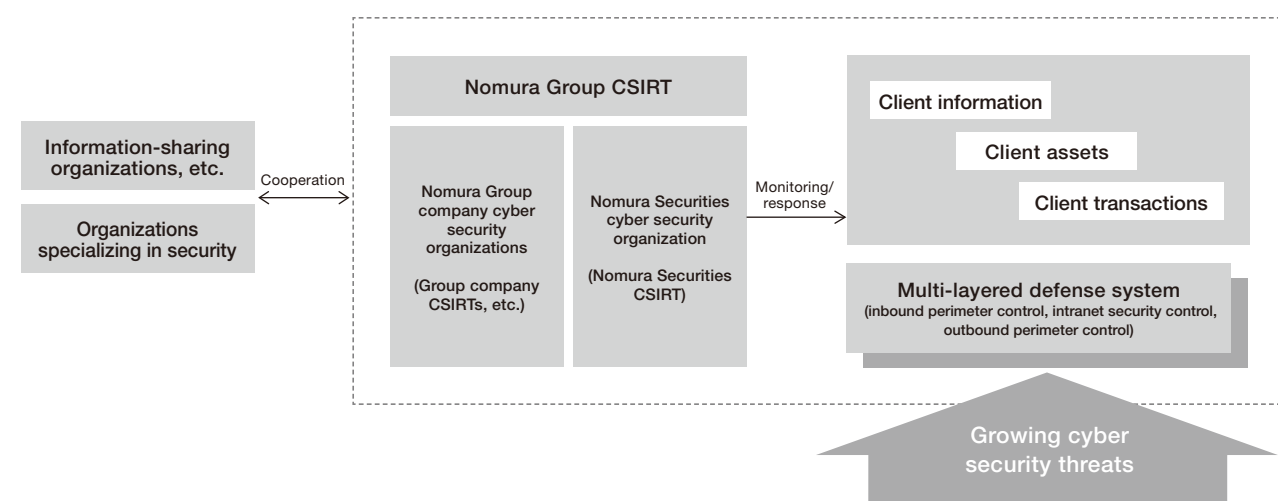


Assessment of the impact on Nomura's earnings of a large-scale natural disaster (Example: earthquake directly under the Tokyo metropolitan area)

Cyber security measures

Nomura Group has for some time been undertaking various security measures to protect systems against cyber-attacks. However, in light of the growing cyber security threat worldwide, we recognize that our current countermeasures may be insufficient.

Faced with this growing cyber security threat, Nomura Group is working continuously to strengthen its cyber security platform to ensure that clients' information and assets are secure, and to enable clients to conduct transactions with peace of mind.



Organizational Structure

Nomura Group, along with Nomura Securities and other Group companies, has established an organizational structure, centered on the Nomura Group Computer Security Incident Response Team (CSIRT), to work together to deal with events stemming from cyber-attacks and to minimize the damage they may cause.

Countermeasures

Recognizing the importance of cyber security amid increasingly sophisticated and cunning cyber-attacks, we established CSIRTs with the aim of further improving our response capability. We are promoting measures to enhance cyber security centering on the way the organization operates, system security measures, executive and employee training, and cooperation with external organizations.

With respect to the organization, we participate in drills to protect against cyber-attacks, and have outside cyber security experts evaluate the effectiveness of our cyber security measures. In addition, when we obtain information on dangerous vulnerabilities or detect cyber security events, the CSIRT leads the response effort to analyze the cause, minimize damage, and quickly restore systems.

In terms of system security measures, we have put in place 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.

As a human-level response, the Group has prepared the Nomura Group Information Security Policy and regularly conducts relevant training for all executives and employees in order to raise awareness among executives and employees.

Nomura Group has established information collecting and sharing systems relating to cyber attacks and attack methods through information-sharing organizations such as Financial ISAC Japan and Nippon CSIRT Association.

Missions of business continuity

The impacts of earthquakes, typhoons, and other natural disasters as well as the threats of terrorism and other malicious acts are increasing in Japan and around the world. In light of this situation, Nomura Group has established a global business continuity management structure and is continuously enhancing its program through implementations of numerous measures and awareness programs.

Business continuity structure

Nomura Group has established the Crisis Management Committee, which is comprised of officers responsible for crisis management from Group companies worldwide, to prepare for major natural and manmade disasters. With this committee in place, we have developed a business continuity and crisis management structure to cover aforementioned disasters globally.

Should a major office be rendered unable to continue its operations due to disasters, we have set up backup offices allowing us to continue our operations from these alternate locations. Similarly, we have built redundancy into our datacenters so that, in the event of a datacenter outage, critical data

and applications will be protected in a backup datacenter located in a different location. Additionally, we have reinforced our infrastructures, for example, such as installing the power generators. Accordingly, these infrastructures can be used in the event of a single building failure or a wide area disaster, such as a Tokyo Inland Earthquake, to avoid systemic risks and continue or quickly recover high-priority operations that are crucial to the lives of our clients. Similar measures and infrastructure have also been placed at our major overseas offices.

The Office of Crisis Management Committee regularly conducts employee safety confirmation drills, disaster prevention drills, and business continuity drills in Japan to ensure that we are able to respond immediately during the crisis situation. For overseas offices, these activities are carried out by the Business Continuity Management Team. Through these efforts, we are working to foster greater awareness of crisis management and strengthen our ability to respond to emergencies. These structures and measures are stipulated in Nomura Group Crisis Management Regulations.

Activities of crisis and business continuity management

- 1 Strengthening structure for business continuity**
 - Establishment and reinforcement of backup offices
 - Establishment of datacenter redundancy
 - Identification of critical resources
 - Enhancement of emergency communication equipment
- 2 Drills and training**
 - Emergency Command Center activation drills
 - Employee safety confirmation drills
 - Drills based on business continuity plan
 - Initial response drills simulating Tokyo Inland Earthquake
 - Nankai Trough earthquake response training at branch offices
- 3 Strengthening collaboration between Group companies in Japan and overseas**
 - Enhancing information sharing between domestic Group companies
 - Enhancing information sharing among overseas Group companies
- 4 Enhancing business continuity plan**
 - Review and revision of business continuity plan
 - Review and revision of business continuity plan for datacenter outage scenario
 - Review and revision of business continuity plan for Tokyo Inland Earthquake scenario
- 5 Others**
 - Stockpiling of water, food, and other emergency supplies at headquarters, branch offices, and backup offices

Risk Management
<http://www.nomuraholdings.com/company/risk/index.html>