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 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.

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.
It is important for us to maintain capital adequacy and achieve business plans under any type of economic environment, to protect our clients, and to comply with laws and regulations.
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.
Our Risk Appetite Statement and risk appetite are approved by the Executive Management Board, and the risk is monitored daily against a set of risk appetite. If by any chance risk amount exceed risk appetite, the senior management consults with stakeholders and takes actions to solve such excess.

Setting risk appetite and guidelines for:

Capital adequacy and balance sheet measures	to comply with capital regulations imposed on financial institutions and to maintain a strong financial base in continuing to conduct businesses under various economic conditions.
Liquidity risk	to maintain sufficient liquidity to survive a severe liquidity situation and to comply with regulatory requirements.
Market risk and credit risk	to manage market risk and credit risk within wholesale businesses.
Operational risk	to understand and mitigate the impact and likelihood of operational risk events assumed in the course of conducting business.
Compliance risk	to promote proper understanding and compliance with the letter and spirit of all applicable laws, rules and regulations and avoid misconduct.

Key risk types

Risks taken by Nomura Group differ by divisions or businesses. We have established a risk management framework based on risk profiles.
Nomura Group has adopted a multi-faceted risk evaluation process to avoid risks that may be damaging to our reputation.

Risk management approach at Nomura Group

Implemented frameworks to evaluate and control the possibility of risks arising from the firm's operations and transactions.

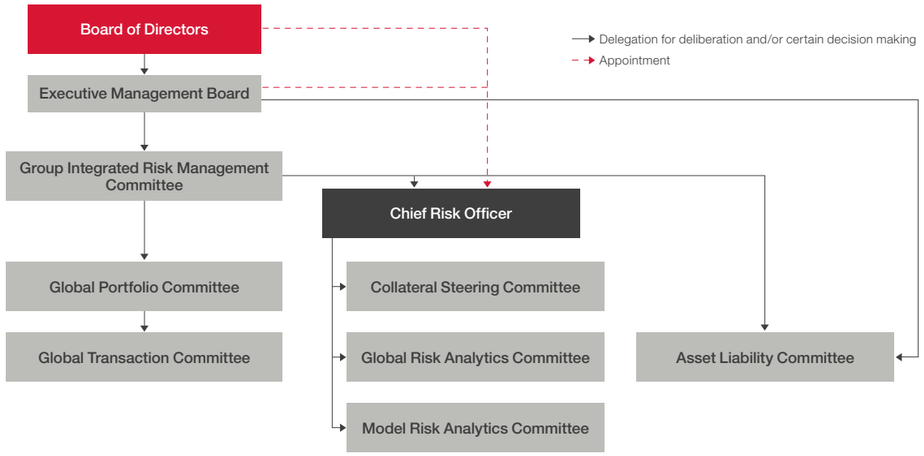
Quantifying risks as much as possible.

Taking a prudent approach to risks which are outside the area of experience and knowledge, and those that are difficult to control by hedging or other mitigating actions.

Division/Business		Retail	Asset Management	Wholesale	Corporate	Other subsidiaries
Selective risk taking	**Market risk** Risk of loss in the value of financial assets and liabilities, as a result of market move in risk factors including interest rates, foreign exchange, and price of securities.		●	●		●
	Credit risk Risk of suffering losses when a borrower is unable to make payment and fail to meet a contractual obligation.	●	●	●		●
Unavoidable risks	**Model risk** Risk of loss arising from model errors, incorrect or inappropriate model application with regard to valuation models and risk models.			●	●	●
	Liquidity risk Risk of losses arising from a potential lack of access to funds or higher cost of funding than normal levels due to deterioration in Nomura's creditworthiness or deterioration in market conditions.			●	●	●
	Operational risk Risk of suffering losses due to internal administrative processes, people, or systems being either inappropriate or not functioning properly.	●	●	●	●	●
Risks that must not be taken	**Compliance risk** Risk that can lead to administrative punishment, economic losses, and reputational damage when Nomura executives or employees violate laws and regulations. Compliance risk also includes risk of losses caused by violating Nomura Group's Code of Ethics and other internal policies and guidelines, including harassment.	●	●	●	●	●

Risk Management Governance and Oversight

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



Key Committees

Group Integrated
Risk Management Committee (GIRMC)

- Upon delegation from the Executive Management Board (EMB), the Group Integrated Risk Management Committee deliberates on or determines important matters concerning integrated risk management of Nomura to assure the sound and effective management of its businesses.
- GIRMC establishes Nomura's risk appetite and a framework of integrated risk management consistent with Nomura's risk appetite.
- GIRMC supervises Nomura's risk management by establishing and operating its risk management framework.
- GIRMC reports the status of key risk management issues and any other matters deemed necessary by the committee chairman to the Board of Directors and the EMB.
- Upon delegation from the EMB, the GIRMC establishes the Risk Management Policy, describing Nomura's overall risk management framework including the fundamental risk management principles followed by Nomura.

Asset Liability Committee (ALCO)

- Upon delegation from the EMB and the GIRMC, the ALCO deliberates on, based on Nomura's risk appetite determined by the GIRMC, balance sheet management, financial resource allocation, liquidity management and related matters.

Global Portfolio Committee (GPC)

- Upon delegation from the GIRMC, the GPC deliberates on or determines all matters in relation to the management of a specific portfolio, for the purpose of achieving a risk profile consistent with the risk allocation and risk appetite of Nomura. The portfolio consists of businesses and products that fall within at least one of the three following categories: event financing, term financing and asset-based financing.

Global Transaction Committee (GTC)

- Upon delegation from the GPC, the GTC deliberates on or determines individual transactions in line with Nomura's risk appetite determined by the GIRMC and thereby assures the sound and effective management of Nomura's businesses.

Collateral Steering Committee (CSC)

- The CSC deliberates on or determines Nomura's collateral risk management, including concentrations, liquidity, collateral re-use, limits and stress tests, provides direction on Nomura's collateral strategy and ensures compliance with regulatory collateral requirements.

Global Risk Analytics Committee (GRAC) and
Model Risk Analytics Committee (MRAC)

- The GRAC and the MRAC deliberate on or determine matters concerning the development, management and strategy of risk models and valuation models, respectively. The primary responsibility of these committees is to govern and provide oversight of model management, including the approval of new models and significant model changes.

FORM 20-F
https://www.nomuraholdings.com/investor/library/sec/

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

How Stress Testing Works

Case Scenario Serious global financial crisis triggered by the failure of a major financial institution.

Assumption of Stress Scenarios
Impact on the market is estimated by referring to past cases; i.e., "flight to quality" causing stock prices to plunge, government bond yields to fall, the appreciation of the Japanese yen and depreciation of currencies from emerging economies in FX market. In order to increase the feasibility of the scenario, the latest market environment is reflected.

Analysis of Stress Scenarios
Based on the assumption that the case scenario has just occurred, the amount of potential losses from trading activities, unrealized losses on investment securities, significant decline in profits due to the loss of business opportunities, and losses caused by counterparty defaults are calculated.

Adopting to the Management
Examine if the minimum capital adequacy ratio is maintained under the stressed conditions; also consider the level of capital buffers need to be maintained in normal times.

CRO Message

Risk Culture In Nomura

Yuji Nakata
Executive Managing Director, Chief Risk Officer

Risk is the possibility of suffering unexpected losses caused by any number of reasons. Risks always lurk behind all business activities. Risk management is about getting ahead of the game by estimating the possibilities of "unexpected" things to happen, and preparing for their impact. It's similar to a physical checkup; checking your vital signs and analyzing data to predict the likelihood of developing a disease, and treating or preventing it as needed. At Nomura Group, we strive to eliminate "unexpected" by analyzing quantified risks and using various measures, including stress tests, to devise contingency plans.
However, it is difficult to eliminate "unexpected." It happens when it happens. Why is that? For one thing, there may be no data to analyze, or too little data to make accurate projections. Another is, that even if the "unexpected" had been expected to some extent, we may have decided that it would not occur or have little impact, and may have lost the flexibility to assume all possibilities.
The business environment is constantly changing, and risks are becoming more diverse and complex. For example, as a result of the globalization of economic activity, the political situation of a certain country can affect the entire world. The rapid digitization of business has led to a complicated and sophisticated cybercrime. We are now entering an era in which "unexpected" is social norm. In other words, the probability of facing "unexpected" may be even higher than ever before.
There is no perfect answer to the question of how should we deal with "unexpected." However, the best way to manage risk and minimize losses is, to use our imagination as much as possible, to know what is likely to happen, how much impact it will have, what preparations we have made, and what is the best way to deal with the "unexpected" should it occur.
At Nomura, we will make full use of our imagination, be prepared well in case of emergency, and strive to be a flexible organization capable of responding to changes in the times and environment.

Cyber security measures

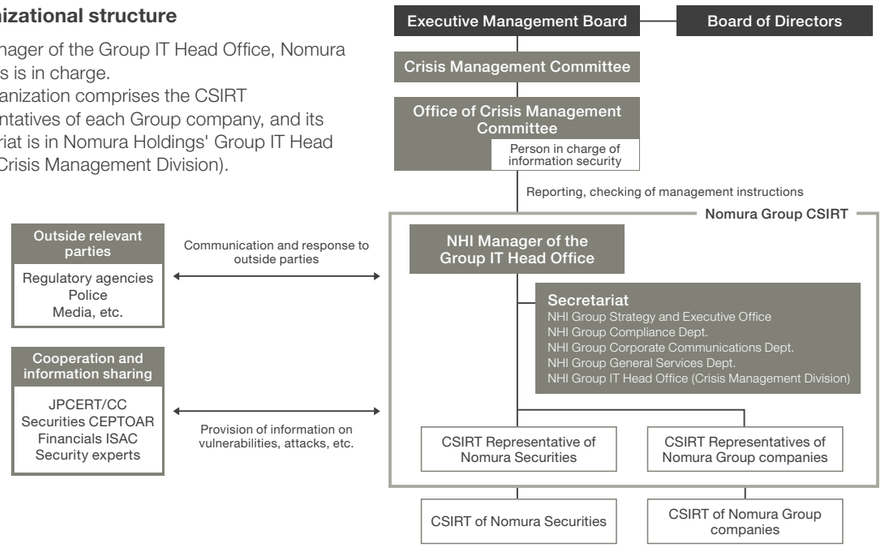
Nomura Group has for some time been undertaking security measures to protect systems against cyber-attacks. However, in light of the increasingly serious cyber security threats throughout the world, we recognize that our current countermeasures may not be sufficient in the future. In addition, in the 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 (Crisis Management Division).



Organization management	At normal times, we take part in cyber security drills, conduct Threat-Led Penetration Test 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 Group is working to build a system for gathering and sharing information on attackers and their approaches through communication with Financials ISAC Japan, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and other information sharing bodies as well as with cyber security vendors.