Nomura Group promotes integrated risk management as part of the firm’s management strategy to control various risks inherent in daily operations, secure capital soundness in any economic environment, achieve business plans, protect customers and comply with laws and regulations.

Risk management policy

All executives and employees of Nomura Group, irrespective of their function, actively engage in risk management. Nomura Group aims to identify the risks that could lead to significant losses by categorizing the types of risks associated with its business activities, as well as the impacts of risks and their likelihood of occurrence. In principle, Nomura Group avoids risks that are difficult to identify and manage. Nomura Group recognizes that there are risks that cannot be identified at present. As financial professionals, all executives and employees of Nomura Group must expand their knowledge of risks, and foster a corporate culture that appropriately recognizes, evaluates and manages risks.

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.

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.

Departments engaged in risk management establish frameworks to manage each type of risk, and support risk management measures taken by the First Line of Defense, such as sales and trading departments.

Departments engaged in risk management independently monitor risks, and keep trading and sales departments in check as needed.

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.

Risk management activities

Based on the concept of PDCA cycle (Plan, Do, Check and Action), all executives and employees of Nomura Group conduct risk management activities as three defensive lines to ensure that the various risks inherent in daily operations do not exceed the level of risk appetite.

Plan

In order to realize Nomura Group’s corporate philosophy, the Executive Management Board formulates business plans and establishes risk appetite taking into account the business environment and the state of management resources. These are reviewed annually or as needed.

Do

Each business division carries out its business plans in accordance with the risk appetite and the Code of Conduct.

Check

The first line of defense identifies, assesses and manages risks that may exceed the risk appetite, as well as carries out activities based on the advice, support and checks received from the second line of defense.

Action

Each business division works to improve risks that may exceed the risk appetite, as well as carries out activities based on the advice, support and checks received from the second line of defense.
Risk Management

Nomura Group’s portfolio of financial instruments includes the following risks. Nomura Group manages these risks by (1) setting the financial risk appetite, Nomura Group classifies market and credit risks into segments according to the nature of business, and uses quantitative metrics or qualitative indicators as well as processes to capture these characteristics.

Non-financial risks exist in daily activities and processes, and can result in a financial loss or significant adverse impact on Nomura Group, our clients and financial markets. It is therefore everyone’s responsibility to manage non-financial risks in line with Nomura Group’s risk appetite.

Non-financial risk

Non-financial risk includes Operational Risk and Reputational Risk.

Operational risk

Risk of financial loss or non-financial impact arising from inadequate or failed internal processes, people and systems, or from external events. Nomura Group’s approach to operational risk management includes four core processes: operational risk event reporting, risk and control self assessment (RCSA), monitoring using key risk indicators (KRI), and scenario analysis. Managed operational risks are divided into the 10 categories below.

Compliance risk

Risk of financial loss or reputational damage due to violations of financial services laws, rules or regulations, and improper conduct which disrupts the integrity of the financial markets and causes unfair client treatment.

Legal risk

Risk of financial loss or reputational damage due to (i) ambiguity and/or insufficiency in contractual terms to secure Nomura’s legal rights and/or enforceability of the contractual terms; (ii) failure to comply with applicable laws and regulations; and/or (iii) failure to adopt to changes in laws and regulations.

IT and Cyber Security

Risk of financial loss or reputational damage due to (i) poor performance or unavailability of IT systems; (ii) data corruption and/or; (iii) unauthorised or improper access to IT systems and data from within or outside the institution.

Business Resilience

Risk of financial loss or reputational damage due to inability to resume normal business operations during a business disruption event and damage to or unavailability of physical assets from natural disasters and other events.

Third-Party

Risk of financial loss or reputational damage due to failure of third-party to perform in line with expectations.

Financial Reporting & Tax

Risk of financial loss or reputational damage due to material misstatement or omission in the firm’s (i) external financial reporting, regulatory reporting or internal financial management reporting; and/or (ii) external tax reporting or payments.

People

Risk of financial loss, staff impact or reputational damage due to acts inconsistent with employment or health and safety laws or employment norms and agreements.

Transaction Lifecycle

Risk of financial loss or reputational damage due to failures in transaction processing and/or process management.

Prudential Risk Frameworks

Risk of financial loss or reputational damage due to inadequate prudential risk management frameworks.

Fraud

Risk of financial loss or reputational damage due to intent to defraud, misappropriate property or conduct unauthorized activity by an internal or third party.

Reputational Risk

The possible damage to Nomura’s reputation and associated risk to earnings, capital or liquidity arising from any association, action or inaction which could be perceived by stakeholders to be inappropriate, unethical or inconsistent with Nomura Group’s values and corporate philosophy. All personnel must consider the impact of their actions or inactions on Nomura’s reputation and apply high standards to their behavior as set out in the Nomura Group Code of Conduct.
Nomura has established an organizational structure to facilitate effective business operations and management of risks.

- **Executive Management Board (EMB)**
  - Executive Management Board deliberates on and determines the Risk Appetite, in addition to the Business Plan and budget.

- **Group Integrated Risk Management Committee (GIRMC)**
  - Group Integrated Risk Management Committee establishes a policy and a framework of our risk management.

- **Chief Risk Officer (CRO)**
  - Chief Risk Officer is responsible for supervising the Risk Management division and maintaining the effectiveness of the financial risk management framework.

- **Chief Financial Officer (CFO)**
  - Chief Financial Officer is responsible for supervising Finance division, and overall financial strategy and liquidity management.

- **Chief Compliance Officer (CCO)**
  - Chief Compliance Officer is responsible for supervising the Legal, Compliance and Controls division ("LCC") and maintaining the effectiveness of the non-financial risk management framework.

**Risk Management, Finance and LCC divisions**

Risk Management, Finance and LCC divisions comprise various departments established independently from Nomura’s business divisions. These three divisions are responsible for establishing and enforcing risk management policies and regulations, establishing and operating risk management processes, verifying the effectiveness of risk management methods, and reporting to Officers and Group Integrated Risk Management Committee.

---

**Internal Audit (Third line of defense)**

In order to ensure the effectiveness and appropriateness of internal controls, we have established dedicated internal auditing departments in the Company and its major subsidiaries that are independent from the execution of business operations, and these departments conduct internal audits in Nomura Group. To ensure the independence of the Internal Audit department from business execution functions, the formulation of the implementation plan and budget for internal audits are subject to the approval of the Audit Committee or the Audit Committee members appointed by the Audit Committee. The appointment and dismissal of the head of the Internal Audit Division requires the consent of the Audit Committee or the Audit Committee members appointed by the Audit Committee.

In order to ensure appropriate corporate behavior throughout the Group in an effort to deliver management transparency, ensure efficiency, comply with regulations, manage risks, maintain the reliability of business and financial reports, and encourage appropriate information disclosure, we are working to strengthen and enhance our internal control system. Important matters in regard to internal controls including internal audit activities is deliberated at the Internal Controls Committee, which is chaired by Group CEO and includes a member of the Audit Committee, and the matters discussed at the Internal Controls Committee are also reported to the Board of Directors.

**Internal Controls System Framework**

Audit Committee actions in relation to large losses with a US client transactions

Audit Committee received a report on the large losses with the US client transactions (during March 2021) immediately after the discovery at the end of March, and decided to conduct an internal investigation as well as a comprehensive review by employing an external law firm. Audit Committee also noted that, as a result of these investigations, we have already implemented emergency preventive measures and we are conducting a comprehensive review by third-party risk management experts on our risk management framework for the Wholesale division and our Risk Management function. Both Audit Committee and Internal Controls Committee will continue to monitor the progress of these actions.

---

*For further details, please refer to our annual report/20F.*