
# RISK MANAGEMENT

**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 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

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.

## Three lines of defense

All executives and employees of Nomura Group actively engage in the risk management through the three lines of defense framework.

1 First line of defense | 2 Second line of defense | 3 Third line of defense

**1 Departments engaged in trading and sales**

As a risk owner, the first line identifies, assesses, and manages risks arising in the course of daily operations in accordance with the Risk Appetite Statement, company policies, and procedures.

**2 Departments engaged in risk management**

The second line is responsible for establishing the risk management framework and supporting the first line. The second line independently monitors risks and reports to senior management. As necessary, the second line controls the first line's risk-taking activities.

**3 Internal Audit Department**

The third line examines the operations and governance of the first and second lines and advises on improvement.





About Nomura 001 | Strategies for Value Creation 005 | Strengths Supporting Value Creation 041 | Corporate Information / Data 079

## Risk appetite

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 levels of risk (risk appetite) that the firm is to take, as documented in the Risk Appetite Statement.
Our Risk Appetite Statement is approved by the Executive Management Board, and risks are monitored daily against the risk appetite.
If by any chance risk levels exceed the risk appetite, senior management consults with those directly involved and takes actions to eliminate excessive risk as necessary.

## Categories for which risk appetite is established

| | |
|---|---|
| Capital adequacy and liquidity | Nomura Group defines the level of capital adequacy and sound liquidity as risk appetite, taking into account the regulatory requirements, funding capacity, and business environment. |
| Financial risk | Nomura Group allocates financial resources to each business in order to achieve corporate strategies and business plans, while remaining within the bounds of the risk appetite forcapital adequacy and liquidity.<br>Nomura Group defines the types and levels of financial risks that each business takes within its allocated resources as financial risk appetite.<br>In 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 risk | 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. |

## Nomura Group's major financial risk

| | |
|---|---|
| Mark to market risk | Risk of incurring losses due to a change in the value of assets or liabilities resulting from movements in interest rates, currencies, and prices of stocks and other securities |
| Market liquidity risk | Risk that trading costs will increase due to the time taken to close positions, or that trading will become unfeasible due to rapid changes in the market. |
| Default risk | Risk of incurring losses when a counterparty or issuer fails to meet its obligations. |
| Event risk | Risks inherent in specific financial transactions, such as losses from events caused by discontinuous changes in the market. Events may or may not result from fluctuations in financial markets. |
| Model risk | Nomura Group uses models for valuation of financial instruments, for measurement of key risks including Value at Risk and counterparty exposure, for estimating liquidity, and for asset price verification.<br>Model uncertainty due to simplification, incorrect use of a model, or reduced model suitability in the current market environment can lead to financial losses and failure to satisfy regulatory requirements.<br>This is called model risk. |

### 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.

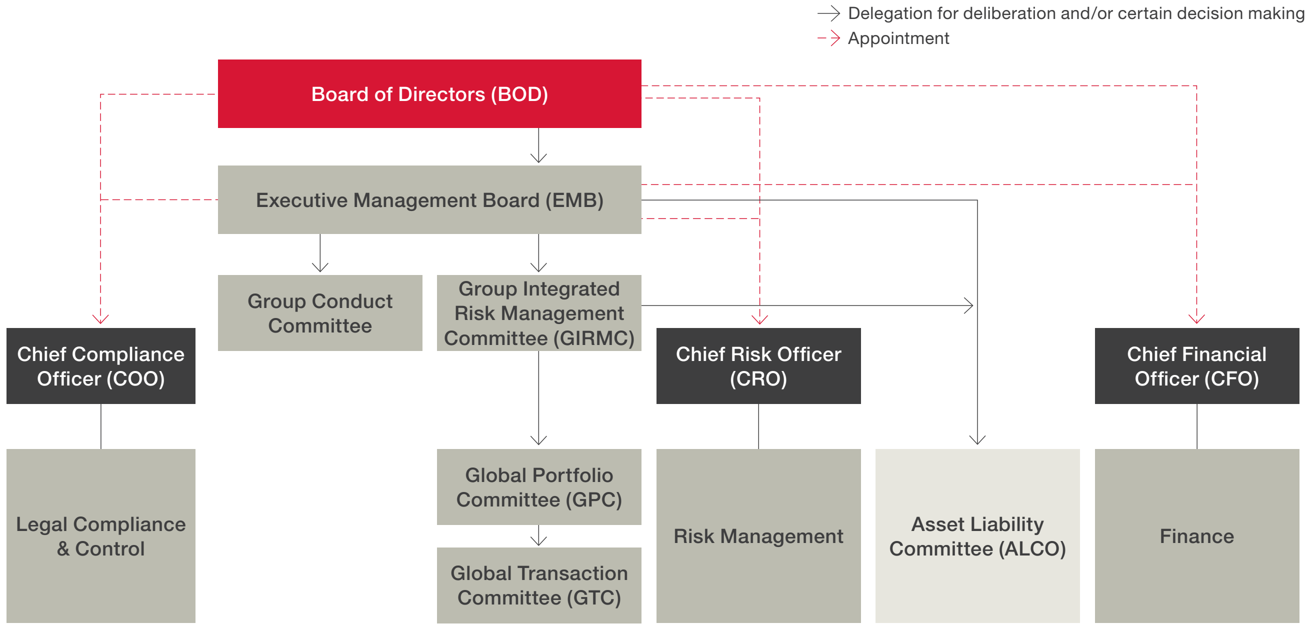
| Risk Category | Definition |
|---|---|
| Compliance | Risk of financial loss or reputational damage due to violations of financial services laws, rules or regulations, and improper conduct which disrupts the integrity of the financial markets and causes unfair client treatment. |
| Legal | Risk of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

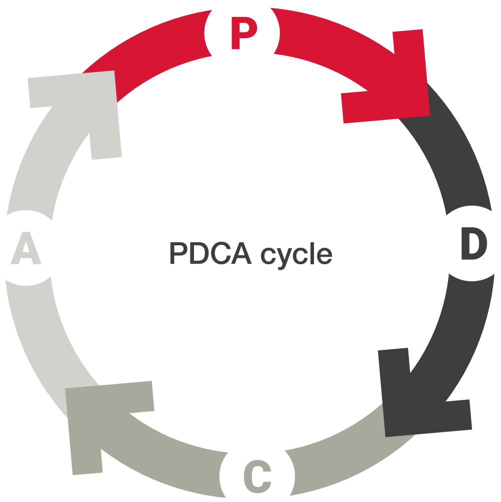
### Risk management governance and oversight

Risk management oversight is carried out by the committees comprising members of senior management. The Group Integrated Risk Management Committee, for example, deliberates and decides on risk management issues material to the firm.




### 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 or committees 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, and the second line of defense advises, supports and checks the first line of defense through monitoring, analysis, stress testing and predictive management. The third line of defense examines and advises on these from an independent position.

**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.