Risk management

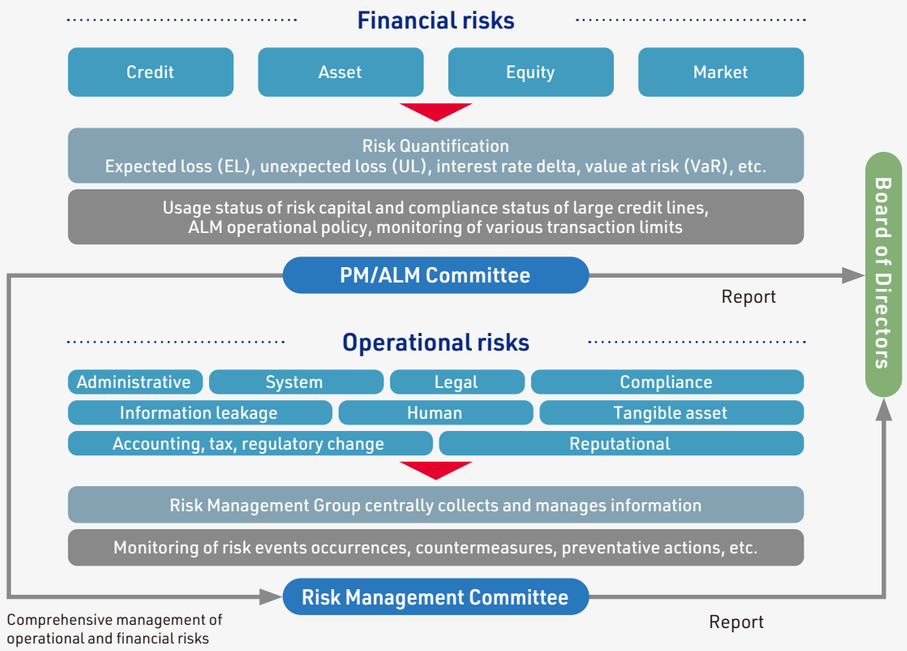
Message from the Head of Risk Management Group

As our group's business continues to diversify and become more sophisticated, the risks arising from our involvement in various projects and business development have also become increasingly diverse and complex.
Under these circumstances, we recognize that appropriately identifying and managing relevant risks according to diverse business strategies and characteristics is crucial for enhancing sound management and corporate value. We are therefore working to strengthen and enhance our risk management framework. We will keep promoting a healthy risk culture in the future by communicating carefully and striking a balance between taking and controlling risks. By doing this, we will promote the development of risk-return management and the efficient use of capital to support the expansion of our group.

Managing Executive Officer
Head of Risk Management Group
Hiroya Uchimura

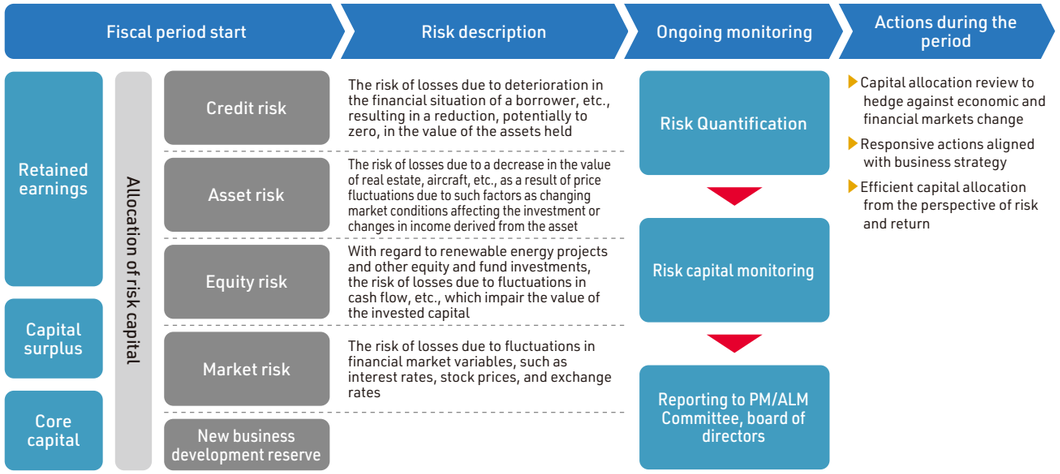
Risk Management Structure

To ensure that we accurately detect, analyze, and control risks related to our business activities and reduce their impact on the company's management, the head of the Risk Management Group oversees and promotes risk management from a companywide perspective. A system has been established to respond quickly and flexibly to risk events via organizations in charge of specific risks according to class and scope.
The group categorizes the risks that arise in the course of business into financial risks, which are managed quantitatively, and operational risks, which are managed qualitatively. It has established a risk management system for each category. In addition, meetings of the PM/ALM Committee and Risk Management Committee are convened with the goal of enhancing risk-related communications and reporting the status of risk management to the Board of directors.



Financial Risk Management System and Risk Capital Allocation

In order to comprehensively understand and control financial risk, we operate under a "risk capital allocation" framework, and we are working to maintain business stability and improve profitability at the same time.
Specifically, we manage each quantified risk in an integrated and centralized manner, keeping the total amount of risk within a certain range of our capital, and we have a system in place that allows us to take risks in a rational and efficient manner within the allocated risk capital for each risk category
During the annual business planning exercise, the board of directors sets the Risk Capital Allocation Plan, which governs how much risk capital is allocated to each risk category. Risk is measured and reported to the board of directors as part of the monthly update on the status of business operations.



*Please also refer to page 91, "Business Risks."

Operational Risk Management

The Risk Management Group centrally collects and manages adverse operational events caused by deficiencies and clerical errors, compliance issues, inappropriate business practices, system failures, and external factors, and takes appropriate measures for each risk category. These may include formulating countermeasures and procedures to prevent recurrence. The status of any such risks is reported to the Risk Management Committee and the board of directors.

Company-wide Response to Cyber security Risks

Our group views the increasing cyber security risks as one of the important management issues and is strengthening company-wide responses. The risk management framework, including the group-wide response policy, responsible parties, management structure, and the duties and responsibilities of pertinent staff, has been clarified, and we have specifically designed a basic policy for cyber security risk management. Additionally, we are strengthening measures to enhance early detection and defense capabilities against cyber attacks. This includes implementing monitoring systems by specialized teams such as the Computer Security Incident Response Team (CSIRT) and Security Operation Center (SOC), deploying multi-layered defenses, and adopting zero trust frameworks, all in collaboration with external experts.
For employees, we are working to enhance their response capabilities through joint cyber security training (pictured) across the Mizuho Lease Group and to raise security awareness through e-learning.

Information Sharing and Action Plan Discussion at the Emergency Task Force Meeting (Exercise)