

Risk Management Policy

As the risks associated with banking operations become increasingly varied and complex, the Bank has formulated a set of internal management policies that take into consideration the Bank's strategic targets in order to ensure that the manner in which it manages its business is both sound and pertinent. Guided by these policies, the Bank works diligently to manage risk.

In specific terms, the Bank classifies the risks it should manage as (1) comprehensive risks; (2) credit risks; (3) market risks; (4) liquidity risks; and (5) operational risks (including administrative and system risks). The Bank conducts appropriate risk management according to risk characteristics.

Management Structure by Type of Risk

(1) Comprehensive Risk Management

In order to appropriately manage the wide variety of risks on a comprehensive basis, the Bank has developed and established a management structure by setting up the Comprehensive Risk Management Department. The Comprehensive Risk Management Department puts in place rules and criteria for determining the scope of comprehensive risk management, management methods, evaluation of new products and operations as well as the level of acceptable risk after taking into consideration management strategies, management capacity as well as business scale and characteristics. Based on these rules and criteria the ALM (Asset Liability Management) and other appropriate committees monitor and control risks. The results of these activities are reported to the Board of Directors and other relevant bodies on a regular basis.

(2) Credit Risk Management

Musashino Bank has historically taken steps to maintain the independence of the Credit Division and to build a stringent screening and management structure in order to maintain and strengthen the soundness of its assets. At the same time, the Bank has adopted a ranking system and endeavored to upgrade and expand its credit risk management capabilities as a part of its efforts to establish objective decisions and lending policies on an individual transaction counterparty basis.

(3) Market Risk Management

Musashino Bank has established the Market Risk Management Department in order to appropriately manage market risks. Relevant steps are taken to ensure the independence of the department from the Market Management Department and Business Promotion Division, and to establish and develop a structure that is capable of harnessing the checks-and-balances function. At the same time, the ALM and Credit Portfolio Management Committees deliberate as and when required.

(4) Liquidity Risk Management

Musashino Bank has established the Liquidity Risk Management Department and Cash Management Department in order to appropriately manage liquidity risk. While ensuring the independence of the Liquidity Risk Management Department from the Cash Management

Department, Market Management Department and Business Promotion Division, every effort is made to establish and develop a structure that is capable of harnessing the checks-and-balances function. At the same time, the ALM Committee deliberates as and when required.

(5) Operational Risk Management

Musashino Bank confronts broad and varied operational risks. For this reason, the Bank classifies risks as (i) administrative risk, (ii) systems risk, and (iii) other operational risks (a. legal risk, b. human risk, c. tangible asset risk, and d. reputation risk), puts in place rules on an individual risk basis and promotes the management of each risk by the appropriate management department. In addition, the Bank has established the Operational Risk Management Department to undertake the management of operational risks on a comprehensive basis. The Bank also pushes forward measures aimed at establishing and developing a management structure that is capable of harnessing the checks-and-balances function with respect to each business division. Moreover, the Operational Risk Management Committee deliberates on issues as and when required.

Crisis Management/BCP Framework

The Bank has established a Business Continuity Plan (BCP) as part of its contingency planning to ensure operations will continue in case of events such as a major earthquake, system disruption, or outbreak of pandemic influenza. The Bank has compiled manuals that establish concrete codes of behavior and countermeasures. In parallel, the Bank holds systematic drills to improve the responsiveness and awareness of all officers and employees. Additionally, the Bank makes improvements to address issues it identifies and related matters, as part of efforts to further increase the effectiveness of the BCP.

Cyber Security Management Framework

We have established the Cyber Security Management Subcommittee as a CSIRT* within the Bank, with the aim of ensuring a highly effective cyber security management framework that includes efforts to prevent cyberattacks and minimizing the damage and achieving an early-stage recovery if there are any such incidents. This subcommittee promotes cross-divisional cooperation among the Bank's divisions that are responsible for systems, risk management, and other areas. Concurrently, the subcommittee remains in close contact with external entities such as the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and police, as well as system providers, via information sharing, discussions, and other means. The subcommittee carries out diverse activities for normal times and for emergencies (should any incident occur).

*CSIRT: Computer Security Incident Response Team

A general term for teams responsible for cyber security management within an organization. At the Bank, the Cyber Security Management Subcommittee and its secretariat are CSIRTs.