Risk governance

Basic approach

To fulfill our responsibility as a global financial institution, the Mizuho group integrates the implementation of risk management with the execution of business strategy and financial strategy through our risk appetite framework, and we advance appropriate risk-taking and risk control in order to grow and develop sustainably together with customers, economies, and society as a whole.

Our basic stance when dealing with risk is to understand its nature, to communicate openly across organizational borders, and to constantly pursue appropriate risk-taking.

Shiro Shiraishi
Senior Executive Officer
Group Chief Risk Officer (Group CRO)

When selecting our top risks for fiscal 2024, in addition to our risk perception with regard to the macro-environment and monetary policy direction in Japan and globally, we discussed the increased focus of society on environmental and social issues such as climate change, loss of nature, and human rights violations, as well as the risks posed by generative AI. We have addressed each top risk with a variety of controls, three of which we will focus on here as they relate to the core topics of the medium-term business plan.

First, our readiness for an increasingly unpredictable global financial and economic environment. With regard to credit risk, we simulate and examine the impact of rising interest rates on the macroeconomy and corporate earnings, and take risks based on an appropriate risk-return calculation. In addition, despite the volatile market environment, with the yen at historic lows against the dollar, we are monitoring trends in different countries' financial policies and working to control market and liquidity risks with a forward-looking approach, drawing on lessons learned from the market volatility caused by rapid interest rate hikes in the US and Europe in recent years.

Second is global risk management. The acquisition of Greenhill in the Americas is an example of our group's expansion of the global CIB business. We are also strengthening our risk management systems in the Americas, EMEA, and APAC to provide banking and securities functions globally.

Finally, we are strengthening our corporate foundations. We must improve readiness in areas of growing risk, such as cybersecurity, and also be vigilant against new risks due to the rapid spread of AI. In order to provide stable financial services, we will strive to improve risk management also from the perspective of operational resilience.

In the context of unprecedented uncertainty around the globe, this will be an important year for us to assess the global environment in a forward-looking manner under our risk appetite framework, and to execute our strategy through flexible and appropriate risk-taking and risk control. We will comprehensively assess and evaluate risks and opportunities in order to proceed with appropriate risk management on a group and global basis.

Top risks

Resurgence of inflation and economic slowdown in the US and Europe	Rising prices, interest rates, and expanding fiscal concerns in Japan	Escalating US-China conflict and sluggish Chinese economy
Global decoupling and growing geopolitical risks	Worsening impact of climate change	IT system failures
Cyberattacks	Money laundering / Financing of terrorism	Improper acts and omissions by executive officers/employees
Stagnation of sustainable growth due to talent shortages	Changes in the competitive environment	

(As of March 2024)

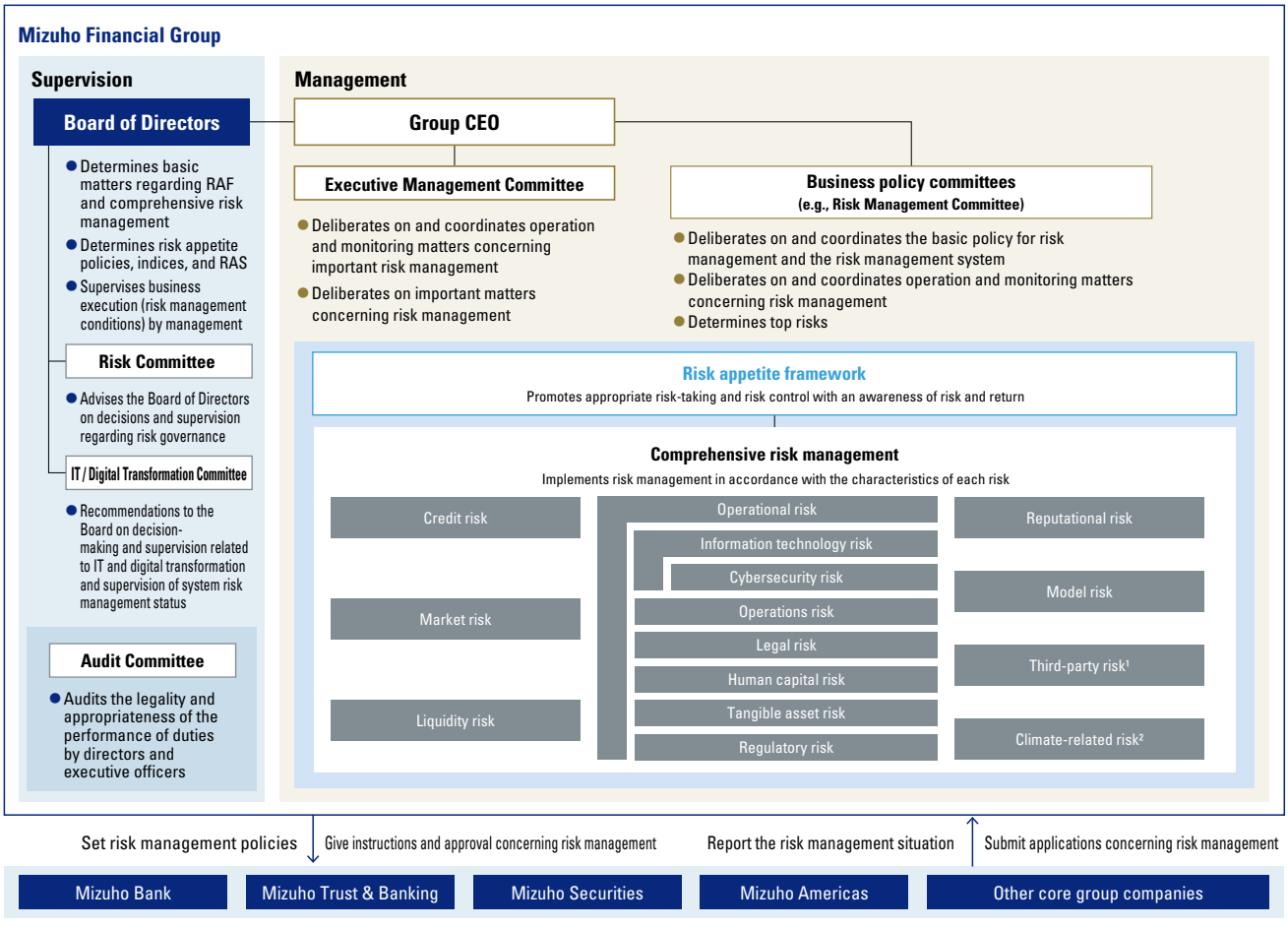
Risk appetite framework (RAF)

We have positioned our RAF as the corporate management framework to execute risk-taking in a manner that is consistent with our risk appetite. Risk appetite refers to the types and levels of risk that we will accept in order to implement our business and financial strategies. Through our RAF, we manage strategy and risk in an integrated manner and aim to achieve the optimal risk and return through appropriate risk-taking and risk control.

In the actual implementation of our RAF, the Board of Directors determines basic matters concerning the RAF and also decides on a risk appetite statement (RAS), which documents the RAF's management system and Mizuho's risk appetite. Operations are supervised based on the Board's decisions. In addition, the Risk Committee, which advises the Board of Directors, provides advice to the Board on matters concerning the RAF and related topics. In business operations, the Group CRO, Group CFO, and Group CSO provide assistance overseen by the Group CEO, and implement business strategy, financial strategy, and risk management from an overall perspective.

Risk appetite is determined through management discussions on top risks and other potential risk events, which are then incorporated into baseline scenarios and risk scenarios that are shared internally. Based on our awareness of these internal and external environments, we then formulate a risk appetite policy consistent with the medium-term and fiscal year business plans. Also, regarding capital adequacy, profitability, and liquidity, we set the quantitative risk appetite indices and their levels. The risk appetite policy as well as the risk appetite indices and their levels are determined by the Board of Directors. The risk appetite operating conditions are regularly monitored and reported to the Board of Directors. The risk appetite is also revised as necessary when there are changes in the environment or strategies.

Mizuho's risk management system



1. Complex risk spanning other risks. 2. Risk that could amplify other risks.

Stress testing

At Mizuho, we assess the suitability of our risk appetite and the validity of our business plans through stress testing, calculating and assessing the financial effect on our capital adequacy ratio and on our performance.

We carry out stress testing based on scenarios formulated taking into account current economic conditions and future outlooks, vulnerabilities in Mizuho's business and finance structures, and other factors. We can confirm whether our capital adequacy ratio, performance, and other indicators are sufficient in the case that stress events actually materialize. If such indicators fall below the necessary level, we reconsider and revise our risk appetite and business plans. In addition, we calculate the impact on risk levels, including interest rate risk in the banking book, and confirm the balance between this risk capital and owned capital at the post-stress stage to assess the adequacy of the capital level.

In addition, to structure robust risk management systems, stress testing is also used to manage risk in various risk categories, such as liquidity risk and market risk.

Mizuho's capital adequacy stress testing

1. Preparing scenarios	2. Calculation of risk impact	3. Analysis and use of results
● Current economic conditions and future outlook ● Vulnerabilities of Mizuho's business and financial structure	● Calculation of the impact on the group upon the risk scenario materializing ● Main items to calculate: Capital adequacy ratio, losses, value at risk (VaR), etc.	● Assessment of the suitability of our risk appetite and our business plans ● Assessment of capital adequacy

Cybersecurity

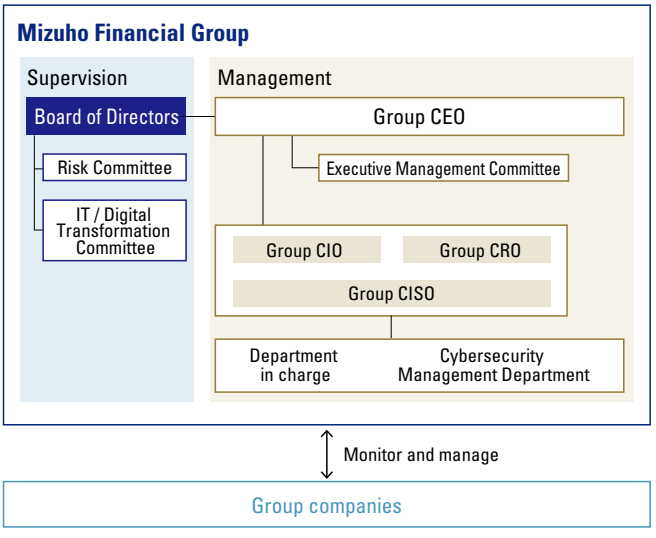
Basic approach

Damage caused by increasingly sophisticated cyberattacks is on the rise. Breaches of personal information held by corporates and a record amount of unauthorized money transfers from phishing are some examples witnessed in 2023. At Mizuho, we are continuously pressing forward with cybersecurity measures as per our Declaration of Cybersecurity Management, to allow customers to use our services with the peace of mind that they are secure.

Declaration of Cybersecurity Management https://www.mizuhogroup.com/who-we-are/activity/cybersecurity

Governance system

At Mizuho, we have established the position of Group Chief Information Security Officer (Group CISO), who administers overall group-wide / global cybersecurity management. In the interest of clarifying how the check-and-balance system applies to the Group Chief Information Officer (Group CIO) as part of our second line of defense, the Group CISO reports to both the Group CIO and Group Chief Risk Officer (Group CRO). We are striving to enhance our cybersecurity posture by implementing this system of double reporting. The Group CISO, as the person responsible for cybersecurity risk management, reports to the Executive Management Committee and Board of Directors the progress of the various measures taken, and works with management to review cybersecurity policies and resource allocation in a timely and appropriate manner.



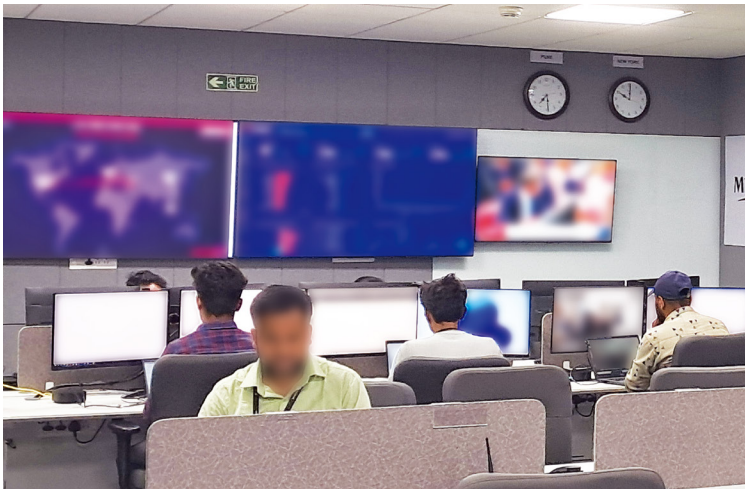
We have appointed a person in charge of cybersecurity and have established a communication system at group companies, to monitor the status of our cybersecurity measures and to quickly gather information when an incident occurs.

Incident response

Our specialist units, particularly SOC[1] and Mizuho-CIRT[2], work closely with external specialized organizations to respond to cybersecurity incidents. SOC detects suspicious activity to identify potential threats using a 24-hour, 365-day monitoring framework, while Mizuho-CIRT shares information with internal and external partners to better handle incident response, investigation, and recovery based on the information received from SOC.

These specialist units have established a procedure for responding to different cyberattack methods, and are constantly conducting internal and external training and drills to properly respond to any incident.

1. Security Operation Center (a specialized team that monitors and analyzes threats to information systems in organizations such as other corporates)
2. Cyber Incident Response Team (incident response teams that specialize in information security issues within the organization)



Surveillance at a location outside Japan

Cybersecurity measures

Our cybersecurity measures include group-wide, global, and supply chain scopes. In order to identify and prevent cybersecurity risks, we collect threat intelligence from public institutions, trusted communities, the media, and other sources, and prioritize measures based on potential impact on our company.

Modern systems are constantly exposed to a wide variety of security threats. We take measures to ensure consistent security throughout the system development lifecycle, from planning through development and operation.

Our systems have a virus analysis and a multi-layered defense mechanism, and we are working to strengthen our resilience by implementing TLPT[1] to test the effectiveness of these technical measures and the effectiveness of the response process.

In order to evaluate the maturity of these cybersecurity measures, we refer to third party assessment by the Cybersecurity Assessment Tool of the Federal Financial Institutions Examination Council and the Cybersecurity Framework of the National Institute of Standards and Technology.

1. Threat-Led Penetration Testing (evaluation of systems and response processes by analyzing targeted threats and simulating attacks)

Cybersecurity personnel development

We periodically test the group's ability to respond appropriately to a cyber incident, and thoroughly eliminate any issues identified. We consider this process vital in order to strengthen individual and organizational incident response capabilities.

To ensure that every executive officer and employee has the necessary cybersecurity awareness, knowledge, and skills, we employ internal and external training, exercises, and drills including incident response training for management and other staff, role-specific cybersecurity training, and biannual phishing email training for all executive officers and employees.

We actively support employees in acquiring professional qualifications and encourage professional development through external specialist programs. In addition, we actively recruit professionals, and have established an IT system course for new graduates hired in Japan, in order to acquire and develop personnel with advanced expertise.