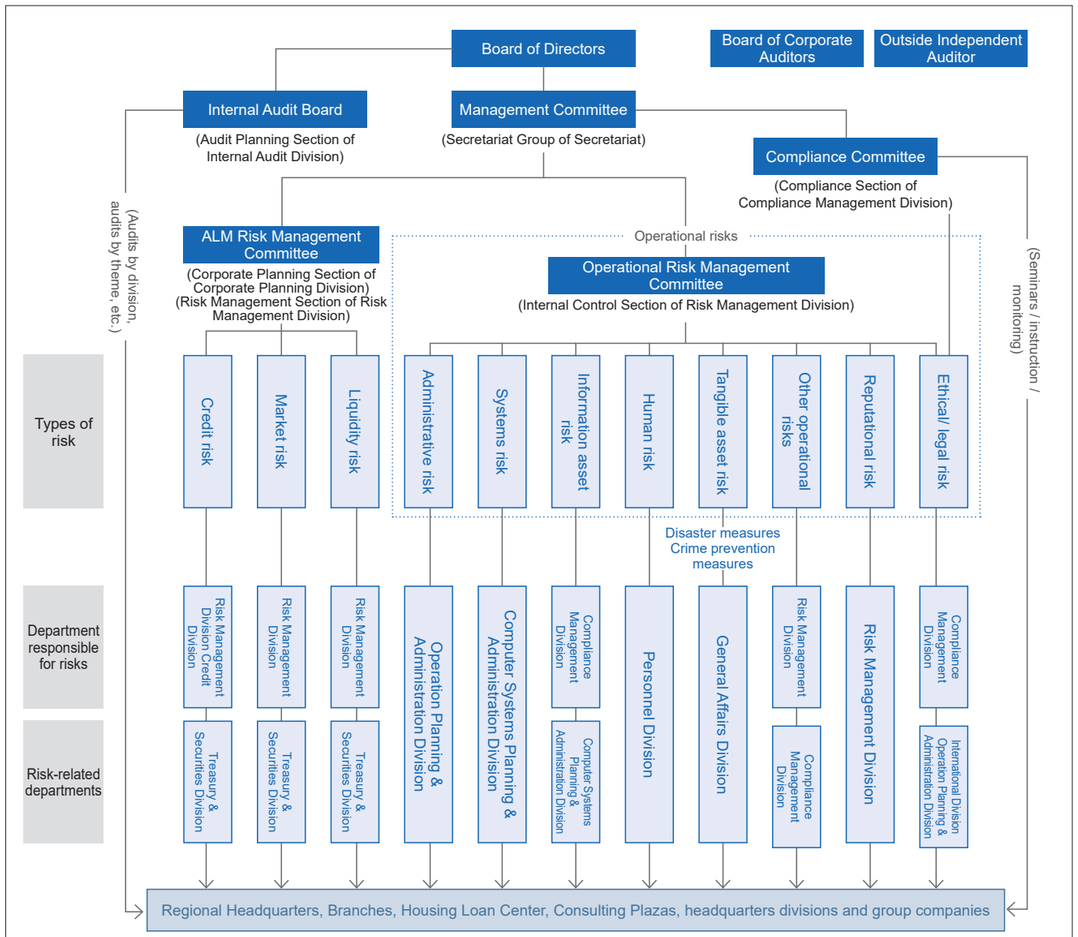
Risk Management

Fundamental risk management policies

With the diversification of financial services and businesses, the importance of risk management is heightening even further. Hyakugo Bank is working to strengthen and enhance risk management with its fundamental policy of establishing an appropriate risk management framework to maintain the soundness and adequacy of management and secure stable income.

Risk Management System



* The Risk Management division refers to the Risk Management Section within the Risk Management Division.

Comprehensive risk management system

Hyakugo Bank has a comprehensive system to understand and manage a variety of risks. Risks are grouped into categories such as “credit risk,” “market risk” and “operational risk.” Some headquarters divisions are designated as having principal responsibility for managing a specific type of risk, and risks are comprehensively managed by the risk management division. In addition, the ALM Risk Management Committee and the Operational Risk Management Committee comprehensively gauge, evaluate and monitor the risks and deliberate on risk management policies and measures.

In addition, based on this comprehensive risk management approach, Hyakugo Bank sets limits for the amount of risk and strives to secure both the soundness and appropriateness of management and stable earnings.

Moreover, by conducting internal audits through auditing units that are independent from business divisions, the Bank has established a mechanism for examining the appropriateness and effectiveness of management within each of its divisions and for encouraging improvement.

Credit risk management

By conducting the appropriate management of credit risk, Hyakugo Bank aims to maintain soundness of assets such as loans and to build a portfolio that has high capital and asset efficiency.

To ensure appropriate returns commensurate with risk, Hyakugo Bank has implemented a credit rating system that employs standardized criteria to evaluate credit risk. In addition, the Bank has established a credit policy that limits the concentration of credit in any specific company or industry, and strives to diversify risk from the standpoint of credit portfolio management.

Hyakugo Bank uses the Foundation Internal Ratings-Based (FIRB) approach to calculate the capital adequacy ratio, and is working on the sophistication of risk management. In internal control, Hyakugo Bank measures and controls credit risk in a way that includes credit concentration risk.

For borrowers facing issues such as deteriorating business conditions, Hyakugo Bank appropriately determines management status and administers guidance for the formulation of revitalization plans as required to resolve problems and recover loans.

Market risk and liquidity risk management

For market risk management, Hyakugo Bank aims to ensure stable earnings while appropriately managing its portfolio and controlling risk at an appropriate level.

Hyakugo Bank mainly uses VaR to quantify various risks such as “interest rate risk,” “foreign exchange risk,” and “stock price risk.”

Hyakugo Bank deals with liquidity risk by appropriately monitoring and managing yen-denominated and foreign currency-denominated cash management. In addition, for contingencies, Hyakugo Bank implements various actions such as securing assets with high liquidity, confirming how much liquidity can be procured in the market, and formulating and implementing measures in advance according to the tightness of credit.

Operational risk management

Hyakugo Bank considers operational risk to encompass a wide range of risks consisting of administrative risk, systems risk, information asset risk, ethical and legal risk, human risk, tangible asset risk, reputation risk, and other operational risks, and is working to upgrade the level of risk management from both qualitative and quantitative perspectives.

Hyakugo Bank also continuously strives to strengthen cybersecurity measures and risk management related to outsourcing.

Crisis management

In addition to these risk management systems, Hyakugo Bank, in light of the public nature of banking operations, has formulated the Business Continuity Plan, which will enable it to continue offering or resume at an early stage the necessary financial services to maintain the social and economic activities of the region, even in the event of a major disaster such as earthquakes or epidemic of new infectious diseases. In addition, Hyakugo Bank is reinforcing its capability to respond to crises by formulating various contingency plans and conducting regular drills.

Cybersecurity measures

To address the increasingly sophisticated cyber attacks in recent years, Hyakugo Bank’s management is committed to staying updated on the latest developments, positioning cybersecurity as an investment and engaging in proactive management.

Basic policy for cybersecurity management	Management will face reality to address the risks, recognize them as key management issues, and take action on their own responsibility while demonstrating leadership.
Scope and level of services to be maintained	We will develop a system that enables us to fulfill our social mission of continuously providing the financial services necessary for sustaining regional social and economic activities.
Risk management system	Management views cybersecurity risks as part of its overall risk management, and has established a system that encompasses all Group companies. A cross-organizational cybersecurity response team, Hyakugo Bank CSIRT*1, has been established to manage both routine and emergency situations, and cybersecurity rules and procedures have been formulated to strengthen the cybersecurity management system. We have also strengthened cooperation with cybersecurity-related organizations by signing a joint response agreement with the Mie Prefectural Police Department and participating in the Financials ISAC Japan*2, an external organization. These efforts facilitate the sharing of information on a wide range of issues and contribute to early warning and preventive measures.
Knowledge of cybersecurity leaders	The Director in charge of the Computer Systems Planning & Administration Division supervises cybersecurity risks as the person responsible for overall cybersecurity. The Director actively participates in training and drills to incorporate external knowledge and strives to update the security system with the latest information. In addition, regular study sessions are held exclusively for the management team to enhance their overall knowledge.
Securing resources	The Bank views cybersecurity as an important part of its internal infrastructure, alongside growth investments, and actively invests in human resources and the development of robust systems. Given the difficulty in attracting skilled external personnel, we will focus on proactive human resource development, such as sending staff to specialized organizations and training them as long-term trainees. We also encourages employees to obtain IT Passport certification and provides training to improve IT literacy across the Group, thereby strengthening the first line of defense in normal times.
Identification of risks and formulation of response plans	We identify and assess cybersecurity risks by gathering threat and vulnerability information from external organizations such as the National center of Incident readiness and Strategy for Cybersecurity (NISC*3), the National Police Agency, and the Financials ISAC Japan, and by conducting periodic vulnerability assessments of the Bank’s information assets. We then systematically take measures to mitigate cybersecurity risks, considering our business environment, management strategies, and risk tolerance.
Emergency response and restoration systems	In preparation for emergencies, we have a system in place to ensure cybersecurity. We also regularly participate in training organized by the Financial Services Agency and other organizations to improve our response capabilities and enable prompt action. In the event of an incident, management will be involved, and relevant departments will be convened to investigate the cause, prevent further damage, and take restoration measures to continue operations and protect information assets.
Incident status	No cyber incidents have occurred to date as unauthorized communications to the Bank’s devices have been blocked.

*1 An abbreviation for Computer Security Incident Response Team, an organization that works in normal times to prepare for the occurrence of potential security events in systems and other areas.
*2 An abbreviation for Information Sharing and Analysis Center, an organization that shares information on cybersecurity countermeasures, etc. among business sectors.
*3 An abbreviation for National center of Incident readiness and Strategy for Cybersecurity, an organization established within the Cabinet Secretariat to provide advice and information necessary for ensuring cybersecurity.