

## Trust from Customers

# Reliability of Financial Infrastructure

To perform its functions as a highly public financial institution, The Norinchukin Bank manages risks that might affect business management appropriately and takes measures to address such risks.

## Risks Surrounding the Bank's Businesses and Measures to Address Such Risks

Today, when Japanese and overseas economic and social situations are changing radically, the risks that could affect business management and operations are increasingly diverse and complicated. Also, an ever-higher level of social demand is seen for customer protection and prevention of fraudulent uses of financial institutions and other scams. Against such a background, the Bank strives to enrich its risk management structure to prevent customers' interests from being harmed unreasonably.

Moreover, given the increasing number of crimes related to deposit and saving accounts, the Bank is promoting measures to ensure the safety of deposits and savings. The Bank has improved its security level to prevent cyberattacks, as well as fraudulent money transfers and withdrawals, etc., in Internet banking. To address customers victimized by such crimes, the Bank responds with sincerity, considering the various circumstances.

Furthermore, to prepare for emergency situations such as the occurrence of a disaster, the Bank implements measures to ensure business continuation such as resuming operation as quickly as possible after such an incident and continuing to provide basic financial services.

## Operational Risk Management

Operational risk refers to a risk that arises in the course of business operations which per se do not generate profit. Operational risk is different from market risk, credit risk and liquidity risk, or the types of risks the Bank actively takes to generate profits. At the Bank, operational risk is further broken down into subcategories, such as processing risk, IT systems risk, legal risk, personnel risk, tangible assets risk, information security risk, business continuity risk, reputational risk and regulatory risk.

For operational risk management, the Bank has established definitions of the risk, its management framework and basic management processes by resolutions of the Board of Directors. In line with these, the Bank has clearly formulated basic policies for operational risk management such as the prevention of large-scale operational risks and has been managing the risk control framework based on such policies. Specifically, for the appropriate management of operational risks that are borne by the Bank's company-wide operations, the Bank has adopted the operational risk reporting system for the collection and analysis of risk events that have come to light, as well as the Risk & Control Self-Assessment (RCSA) system for the evaluation of potential risks applicable to all divisions and branches.

Important issues such as the basic policies and annual planning of the Bank's operational risk management are first discussed at the Risk Management Committee, and then approved by the Board of Directors. The Operational Risk Management Committee, comprised of relevant members of the Board as well as the general managers of related divisions, is set under the Board's supervision, and monitors the current status of the Bank's operational risk management. The committee also promotes cross-risk as well as cross-divisional approaches towards managing operational risk. Furthermore, the Bank has established a division to be in charge of operational risk management, which is independent of the business lines, as well as divisions to be in charge of individual risks. The Bank has also designated a person to be in charge of operational risk management in each branch and division.

## Reliability of Financial Infrastructure

---

### Information Security Initiatives

The Bank utilizes a variety of information obtained during transactions with customers, etc., for various kinds of operations. Amid the increasingly diverse environments and purposes for information handling due to the rapid progress and evolution of information technology, the Bank is focused on information security measures to protect and manage customers' information appropriately.

The Bank works systematically to enhance its information security, centered on the Risk Management Division with overall responsibility for information security planning, promotion and progress management. Also, important matters related to the improvement of the information security management frameworks are discussed mainly at the Operational Risk Management Committee. Especially concerning personal information, the Bank has set out the Personal Information Protection Declaration and has created a framework for the requirements from a Personal Information Handling Business Operator and Person in Charge of a Process Related to an Individual Number to facilitate the proper handling of Personal Information and Individual Number.

### Cyber-Security Initiatives

The Bank recognizes the threat of increasingly sophisticated and intricate cyberattacks as an important managerial risk. Mainly at the core IT & Systems Planning Division in charge of cyber-security, under the cross-division management framework including discussions at management-level meetings, the Bank is strengthening its cyber-security measures. The Bank also has installed a cyber-security–dedicated CSIRT (Computer Security Incident Response Team), which is in charge of addressing a situation at the occurrence of an incident, multi-tier prevention of such incidents, improving detection and monitoring systems, and conducting training assuming that such an incident has just happened.

## The Main Classifications and Specific Management Methods for Operational Risk

Main Classifications		Specific Risk Management Methods
Risks for which the Bank's key management strategy is the prevention of risk event occurrence	Risk in General	<ul style="list-style-type: none"> <li>• In the operational risk reporting system, a comprehensive and clear reporting standard is established, and information of risk events is collected and analyzed.</li> <li>• With RCSA (Risk &amp; Control Self Assessment), processing sections uncover the risks inherent in their own business processes, evaluate the effectiveness of controls and remaining risks, and important matters that require improvement are incorporated into the management plan for the year.</li> <li>• Coordination of the operational risk reporting system and RCSA.</li> </ul>
	Process-ing Risk	<ul style="list-style-type: none"> <li>• The processing risk management plan is formulated based on the results of the operational risk reporting system and processing risk RCSA, and the progress of the plan is reported to the Bank's management periodically.</li> <li>• Ongoing initiatives such as implementing preventive procedures for specific risk events which have surfaced in the past, updating the current procedure manuals, carrying out self-checking exercises and hosting staff training sessions.</li> <li>• Implementing risk assessments that respond to any major environmental changes in the Bank's business environment due to the adoption of new products and services or organizational restructuring, etc.</li> </ul>
	IT System Risk	<ul style="list-style-type: none"> <li>• An IT system risk management plan is formulated based on the results of IT system risk RCSA, etc., while appropriately handling emerging risks generated by changes in the internal and external environment relating to information security, etc., and progress is reported to the Bank's management periodically.</li> <li>• Information on system failures is collected and analyzed, and future prevention plans are formulated. In addition, in order to meet public demands as a social infrastructure for providing stable financial services, we examine system recovery procedures, assuming the occurrence of a major system failure, ensuring that the impact of such failures is kept to a minimum.</li> </ul>
	Legal Risk	<ul style="list-style-type: none"> <li>• Centralized control and response for litigation for the Bank as a whole.</li> <li>• While appropriately dealing with legal consultations from branch offices, gain an understanding of the existence of risks associated with such laws, regulations and contracts that the Bank should be mindful of, then communicate and teach them to branch offices.</li> </ul>
Risks for which the Bank's key management strategy is the mitigation of the impact and effect of risk events following their occurrence	Business Continuity Risk	<ul style="list-style-type: none"> <li>• Establish a business continuity structure for the Bank and cooperative banking business as a whole.</li> <li>• Verify and improve the effectiveness of the business continuity structure by conducting regular drills simulating a major disaster (such as an earthquake with its seismic origin directly below Tokyo or a pandemic of a new contagious disease).</li> </ul>

## Trust from Customers

# Respect for Customers

Always mindful that The Norinchukin Bank's operations are supported by our customers, we take a sincere approach toward our customers and develop systems to address customers' demands.

## To Meet the Needs of Our Customers

The Bank considers it an important role to provide necessary funds smoothly to its customers engaging in agricultural, fishery and forestry operations and SMEs. To meet the needs of customers by offering customer-oriented services, we engage in ongoing efforts to enhance our functions and services with careful attention to customers' requests.

## Sincere Attitude toward Our Customers

As a provider of financial products and services, the Bank regards it as important to seriously consider customer protection with the perspective of a customer and provides information to help customers make appropriate decisions. Especially when we help customers carry out transactions in financial products that require highly-specialized knowledge, it is essential that we make the effort to carefully explain contracts in easy-to-understand language. For that purpose, we have established various committees and set rules and regulations for customer protection.

## Dealing with Consultations and Complaints by Customers

Consultations and complaints by customers are systematically handled by the departments concerned, and liaison and reports are provided according to the rules and regulations for customer support and related services that prescribe the use of financial ADR (Alternative Dispute Resolution) measures to resolve financial disputes out of court.

The Bank's contacts for handling consultations and complaints by customers are widely publicized on its Web site and elsewhere.

### JA Bank Consultation Service Center

JA Bank has internal rules and systems in place to deal with consultations and complaints by customers in a swift, fair and appropriate manner, while considering financial ADR measures. Consultations and complaints by customers are handled through the JA Bank Consultation Service Center, a fair and neutral third-party organization, as well as the relevant avenues at JA (Japan Agricultural Cooperatives) and JA Shinnoren. With the consent of the customer, we urge the relevant JA or JA Shinnoren to promptly resolve the issue. In addition, we address our areas of operation that might need improvement relative to consultations and complaints and take measures to prevent recurrences by uniting all forces of JA Bank.

## Respect for Customers

---

### JF Marine Bank Consultation Service Center

JF Marine Bank has internal rules and systems in place to deal with consultations and complaints by customers in a swift, fair and appropriate manner, while considering financial ADR measures. Consultations and complaints by customers are handled through the JF Marine Bank Consultation Service Center, a fair and neutral third-party organization, as well as the relevant avenues at JF (Japan Fishery Cooperatives) and JF Shingyoren. With the consent of the customer, we urge the relevant JF or JF Shingyoren to promptly resolve the issue. In addition, we address our areas of operation that might need improvement relative to consultations and complaints and take measures to prevent recurrences by uniting all forces of JF Marine Bank.

## Trust from Customers

# Appropriate Business Activities

The Norinchukin Bank constantly strives to establish and maintain a fair business relationship to ensure a long-term relationship of mutual trust with its customers.

### Strict Information Management

Directors and employees of the Bank have access to information concerning customers' assets, credit, privacy, etc. Strict measures are in place to ensure that such customer information is not leaked by the relevant persons while at or after leaving the Bank. Extra care is taken to ensure compliance with the rules and regulations to prevent insider trading when we obtain yet-to-be announced significant facts concerning listed or other important customers.

### Protection of Personal Information

As a Personal Information Handling Business Operator and Person in Charge of a Process Related to an Individual Number, the Bank has created a required framework to facilitate the proper handling of Personal Information and Individual Number. The Bank educates and trains employees.

### Fair Business Operations

The Bank explicitly makes it an important management policy to systematically prevent any inappropriate acts that could lead to a failure to fulfill social responsibilities, such as the Bank or its directors and employees causing damage to customers or damaging the soundness of or fair competition in the financial market, by promoting a sound risk culture throughout the Bank. When investing in financial products, placing system orders and/or purchasing goods and services, we comply with fair market rules and appropriate business practices to ensure fairness and transparency in our relationships with business partners and suppliers. With governmental organizations, we abide by the National Public Service Ethics Act and other relevant laws, rules and regulations to establish and maintain sound and normal relationships without engaging in any entertainment or gift-giving acts designed to provide unfair profits to public servants or other government employees. Regarding entertainment for and gift-giving to customers, we comply with the relevant rules and follow the approval, reporting and other prescribed procedures.