Initiatives for Compliance

Basic Compliance Policies

To fulfill its basic mission and social responsibilities and prove itself worthy of its customers' and members' trust and expectations, the Bank manages its business in accordance with societal norms, for instance, by fully complying with laws and regulations based on the principle of total self-reliance. We are also constantly working to achieve a higher degree of transparency by emphasizing proper disclosure and accountability.
As part of this effort, the Bank has defined its basic compliance policy in its Code of Ethics, Environmental Policy, and Human Rights Policy. In addition, the Bank disseminates the Code of Conduct to all officers and employees to show the criteria for judgment and action to ensure good faith and fair execution of duties as a prerequisite for business operations and advises specific ways of thinking to put the Shared Values into action. These measures will ensure that compliance awareness is thoroughly understood and practiced by all officers and employees as they go about their daily business.
In addition, internal audits are conducted regularly concerning the adequacy of the Bank's efforts, including those to ensure compliance and to instill a sound risk culture. In response to recent growing societal demand for greater customer protection, based on its Customer Protection Management Policy, the Bank has taken steps to reinforce its management systems as part of its compliance efforts aimed at winning customer trust. These steps include providing explanations to customers, handling customer complaints and inquiries, managing customer information, managing contractors in the case of outsourcing customer-related business, and managing transactions that might involve a conflict of interest with customers.

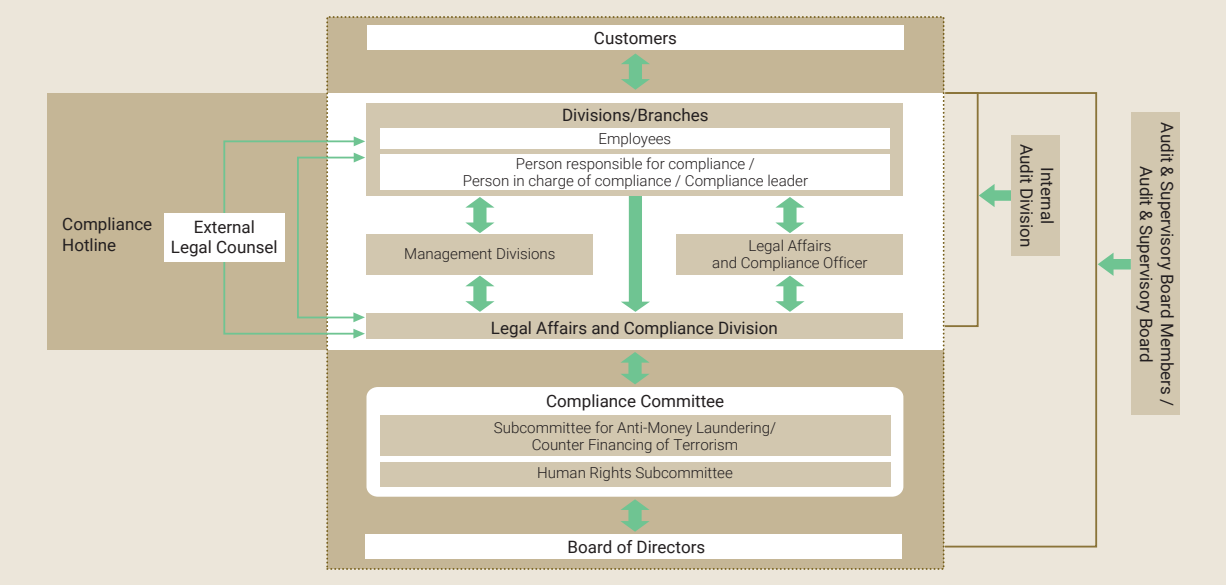
Click the following links to view the Bank's Code of Ethics, Environmental Policy, and Human Rights Policy.

Code of Ethics	https://www.nochubank.or.jp/en/about/ethics.html
Environmental Policy	https://www.nochubank.or.jp/en/sustainability/management/policy/pdf/environmental_policy.pdf
Human Rights Policy	https://www.nochubank.or.jp/en/sustainability/management/policy/pdf/humanrights_policy.pdf

Compliance Activities Directly Linked to Management

The Bank's compliance framework comprises the Compliance Committee, the Compliance Division (Legal Affairs and Compliance Division), and Legal Affairs and Compliance Officer, as well as personnel responsible for compliance, those in charge of compliance, and compliance leaders assigned to the Bank's divisions and branches. The Compliance Committee has been established as a body under the Board of Directors to discuss and determine important matters pertaining to the establishment of the Bank's compliance framework. Important matters discussed by the Compliance Committee and proposals thereof are subsequently approved by or reported to the Board of Directors. The Compliance Committee also treats operational risks, measures against money laundering and terrorist financing, and information security as agenda items, and discusses important policies for executing business pertaining to these topics.
In addition, the Subcommittee for Anti-Money Laundering / Counter Financing of Terrorism and the Human Rights Subcommittee, which are subcommittees under the Compliance Committee, are working to enhance discussions on the compliance framework and strengthen the PDCA cycle pertaining to the operation of the framework.
The Bank also has clarified its efforts to disseminate a sound risk culture and systematically prevent inappropriate behavior as part of its risk handling policy in the RAF.

Compliance Framework



Compliance Practices within the Bank

The Bank's compliance framework at branches and divisions is based on the combined efforts of each employee, primarily centered on the General Manager of each branch or division and other equivalent persons who are responsible for compliance, together with a person in charge of compliance and a compliance leader. Directly appointed by the General Manager of the Legal Affairs and Compliance Division, persons in charge of compliance oversee all compliance-related matters at their branches or divisions. They are expected to handle requests for advice or questions from other members of staff, to organize branch or divisional training and educational programs, and to liaise with, report to, and handle requests to the Legal Affairs and Compliance Division.
Legal Affairs and Compliance Officers appointed in the Food & Agri Banking Business, the Retail Banking Business, the Global Investment and Banking, and the Corporate & Shared Services headquarters support each headquarters' operations from the aspect of compliance.
The Legal Affairs and Compliance Division, supervising overall compliance activities, acts as the secretariat for the Compliance Committee. It strives to strengthen the compliance framework by conducting compliance reviews, responding to requests from branches and divisions for compliance-related advice, and conducting compliance monitoring, which includes visiting branches and divisions to verify their compliance practices directly while providing guidance.

Compliance Program

Each fiscal year, the Bank institutes a Compliance Program incorporating its management frameworks for compliance and customer protection, as well as promotion of initiatives, education, and training plans for them. The Legal Affairs and Compliance Division implements the Compliance Program and monitors its progress to further reinforce the Bank's compliance framework.

Cooperation with Group Companies

To foster and disseminate a sound risk culture throughout the Norinchukin Group, the Bank shares its Code of Conduct with major group companies and provides support for its dissemination and translation to action at each. The Bank is taking steps to strengthen the compliance systems of the entire Norinchukin Group by promoting a common awareness of compliance issues discussed at regular meetings with compliance divisions of its group companies and providing support for formulating and implementing compliance programs and training activities at each group company. Additionally, to reduce compliance risks in the Norinchukin Group, the Bank has established an external contact for consultation on harassment, conducts offsite monitoring at each company (onsite monitoring at some companies), and takes other steps to identify problems as soon as possible.

Whistleblowing System

The Bank has established a whistleblowing system and put in place a Compliance Hotline so that if compliance problems occur, directors, employees, and others can report these either by phone or e-mail.
The Compliance Hotline offers several contacts to report to the Legal Affairs and Compliance Division or outside lawyers while enabling the reporter to choose anonymity or non-anonymity. When an issue is reported to the division, the Bank conducts an investigation, makes necessary improvements, and implements corrective measures. The Bank's compliance operation prioritizes protecting whistle-blowers, for example prohibiting disadvantageous treatment of a whistle-blower and keeping the information of reported content secret, and the Bank makes efforts while striving to improve trust in the system.
In fiscal 2024, although ten cases were reported to the internal and external reporting channels at the Bank, none resulted in a major impact on the management of the Bank.
Notably, each overseas branch has contacts separate from those described above in place to receive reports from employees.

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's Board of Directors has the ultimate responsibility for establishing and maintaining an information security management system. The Bank works systematically to enhance its information security, which is led by the Legal Affairs and Compliance Division with overall responsibility for information security planning, promotion, and progress management, together with the persons responsible for information security (General Managers) and other personnel in charge of information security of each branch or division. Also, important matters related to the improvement of the information security management frameworks are discussed mainly by the Compliance Committee.
Regarding the handling of personal information, the Bank has set out the Personal Information Protection Declaration and has established the security framework that complies with Japanese legal requirements as a Personal Information Handling Business Operator and Person in Charge of a Process Related to an Individual Number as defined under "Act on the Protection of Personal Information." The Bank's policy extends to suppliers (outsourcing contractors) to ensure their appropriate personal information management in case outsourced work involves personal information. Specifically, the Bank's "Basic Policies for Risk Management" stipulates that processes and contractual relationships must be established to ensure the same level of risk management as if the Bank were performing the tasks internally.
The Bank conducts annual e-learning sessions for all employees on information security—including the appropriate handling of personal information—and also provides training at each level of the hierarchy to raise awareness of information security.
Overseas, the Bank has established a privacy policy applicable to the Bank's London Branch and Norinchukin Bank Europe N.V., as well as a privacy policy for residents in the United States.

Cybersecurity

Cybersecurity Initiatives

The Bank is strengthening its cybersecurity measures as it recognizes the threat of increasingly sophisticated and intricate cyberattacks as an important managerial risk.

Basic Policy on Cybersecurity

The Bank has established a basic policy for cybersecurity management in the Basic Regulations on Cybersecurity to minimize the risk of cyber incidents causing damage to the Bank's customers and/or disrupting the Bank's operations or the financial system as a whole.

Cybersecurity Structure

As for organizational structure, we designate the Director in charge of the IT & Systems Planning Division as the "Chief Cybersecurity Officer" to clarify roles and responsibilities regarding cyber risks. Under the supervision of the Chief Information Security Officer, various measures are promoted, led by the IT & Systems Planning Division in charge of cybersecurity.
The occurrence of cyber incidents, threat trends and the status of cybersecurity measures in place are regularly reported to the Board of Directors and other management-level committees such as the Business Infrastructure Committee and the Compliance Committee, which discuss cybersecurity policies.
Within the IT & Systems Planning Division is a team specializing in cybersecurity called the Computer Security Incident Response Team (CSIRT). The Bank's CSIRT works closely with the SOC, or Security Operation Center, which is staffed by an external security vendor, and monitors events that could be a sign of a cyber incident 24 hours a day, 7 days a week, thereby preparing for an initial response when a cyber incident occurs. The CSIRT also collaborates with the government, law enforcement agencies, and various organizations such as ISAC to gather information on cyberattack tactics and new vulnerabilities and to strengthen countermeasures.
Furthermore, to ensure cyber resilience, the Bank established procedures and contingency plans for responding to cyber incidents and confirms the roles and procedures of each department through periodic incident response exercises.

Cybersecurity Management Process

Regarding the confidentiality, integrity, and availability of its information systems, the Bank assesses system risks based on the Security Guidelines on Computer Systems for Banking and Related Financial Institutions and other information from the Center for Financial Industry Information Systems ("FISC"), and implements necessary control measures.
As a cross-organizational cybersecurity management process, the Bank organizes cybersecurity programs in accordance with NIST's Cybersecurity Framework from the perspectives of "identify," "protect," "detect," "respond," and "recover," and reviews necessary measures based on external threats such as changes in attackers' tactics and internal vulnerabilities.
The effectiveness of these cybersecurity management efforts is confirmed through annual internal and external audits, as well as vulnerability assessments and penetration tests.

Education on Cybersecurity

The Bank provides education for different purposes to improve the knowledge and awareness required of each of its officers and employees.

- E-learning for all officers and employees to acquire basic knowledge of security
- Newsletters for presenting cybersecurity-related articles to raise awareness of cybersecurity among all officers and employees
- Suspicious e-mail training for all officers and employees to increase their awareness of and readiness for targeted e-mail attacks
- Lectures by experts to improve the knowledge on cybersecurity of officers
- Incident response training for officers and staff of relevant departments to confirm response procedures in the event of a cyber incident
- Training by external experts to improve CSIRT's forensic skills

The Bank also established an external qualification incentive program to develop cybersecurity specialists and improve their professional skills.

Cybersecurity Structure