Risk Management

GOVERNANCE

Policy and Concept

In accordance with the Kansai Electric Power Group Risk Management Rules established in April 2006, risks that have the potential to affect the achievement of organizational goals are to be recognized and identified. An assessment is subsequently made, followed by implementing necessary measures to deal with the risks. The impact of risk on the Group is being managed at an appropriate level through this series of processes.

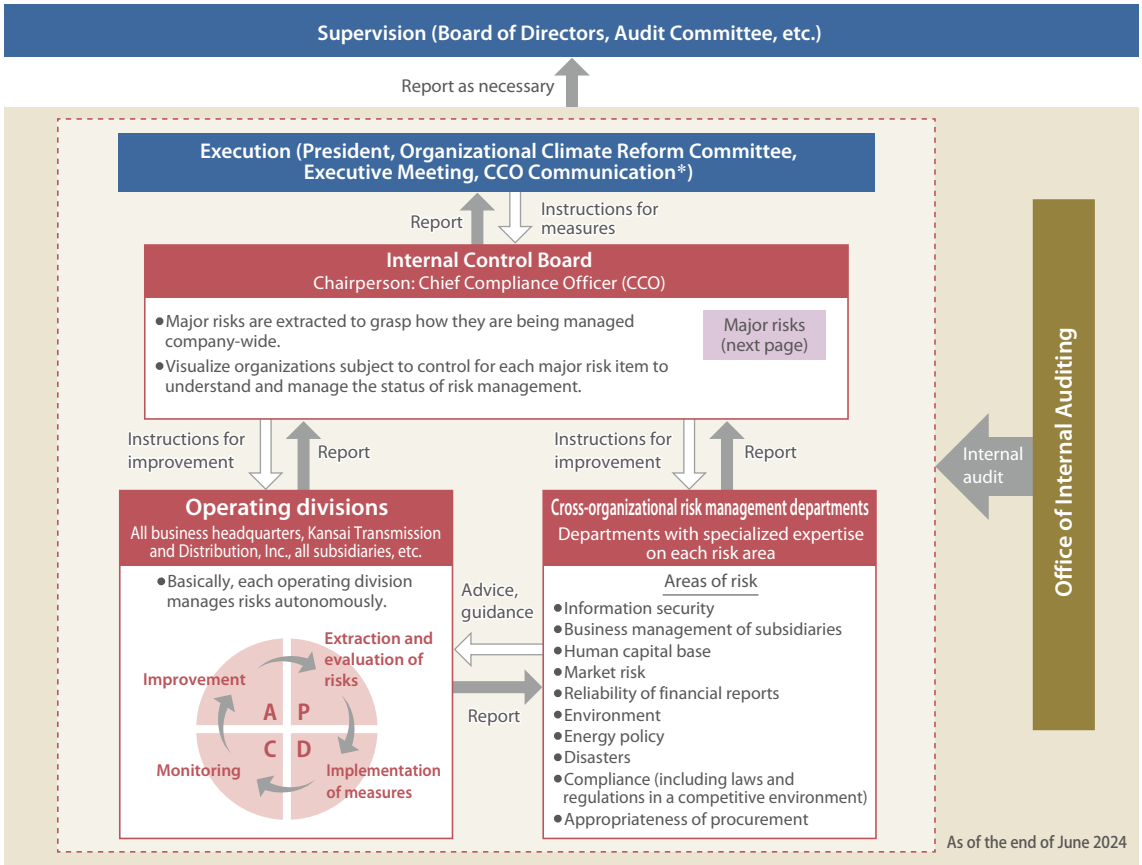
System

Risks associated with the Group's business activities are to be managed autonomously by each operating division. Management of risks considered to have cross organizational importance, such as information security, business management of subsidiaries, human capital base, market risk, financial report reliability, environment, energy policy, disasters, compliance (including laws and regulations in a competitive environment), and appropriateness of procurement, is enhanced by the supervision of departments with specialized expertise in each area of such risks that provide advice and guidance to the operating divisions on an as-needed basis.
The Compliance Promotion Headquarters supports these efforts and centrally promotes compliance, risk management, etc. for the entire Group*.

* See page 125 for a general picture of our compliance promotion system.

Moreover, an Internal Control Board has been established to put risks under central management. The Chairperson of the Board, who also serves as the Head of Compliance Promotion Headquarters (Chief Compliance Officer), is appointed as the Risk Management Officer of the Group, and the Board strives to manage risks associated with the Group's business activities at an appropriate level through this system.
The Internal Control Board oversees risk management plans by, for instance, coordinating cooperation between corporate divisions and operating divisions that have expertise to ensure group-wide risk management. The Board also reports its risk evaluation results to the Executive Meeting and, as necessary, the Board of Directors. If necessary, it improves the structure and system of risk management.
Furthermore, the Office of Internal Auditing conducts internal auditing on the maintenance and operation of the risk management system, and we are working to make improvements based on audit results.

Risk management system



*Dialogue conducted by the Chief Compliance Officer (CCO) with each director to ascertain and evaluate the risk management status in each division

Efforts

The Internal Control Board meetings were held seven times during fiscal 2024 to identify major risks that could greatly affect our Group's business activities. The Board ascertains and evaluates how they are managed company-wide.
From the perspective of effective and appropriate risk measures, these major risks were identified through repeated discussions at the management level, with a focus on each component that affects earnings. The risks were systematically sorted out by business (specific to the electric power business that makes up a large proportion of our business, and common to all businesses) and by factor (strategy, operations, hazard, and finance), and are based on responses to recent risk events such as system failures.
Risks specific to the electric power business include: 《1》 Climate change, 《2》 Nuclear power-related risks, 《3》 Blackout, etc., and 《4》 Delays in responding to rapid changes in the competitive environment. Meanwhile, risks common to all businesses are: 《5》 Changes in laws, regulations, and regulatory policies, 《6》 Stagnation of innovation, 《7》 Damage to asset value, 《8》 Fluctuations in the human capital base, 《9》 Instability or disruption in the supply chain, 《10》 IT governance and information security risks, 《11》 Governance and compliance risks, 《12》 Environmental issues (violation of environmental laws and regulations, etc.), 《13》 Natural disasters, changes in international situations, etc., and 《14》 Market condition / market fluctuation risks.
Classification, major risks, and risk details are shown in the table below.

Major risks

Classification		Major risks	Risk details
Electric power business (energy / power transmission and distribution)	Strategy / Hazard	《1》 Climate change	Risk of delay in promoting zero-carbon emissions and in responding to global warming and other extreme weather events induced by climate change
	Strategy / Operation	《2》 Nuclear power-related risks	Risk of exerting significant impact on local communities, including those with a nuclear plant, and society due to the release of radioactive materials and other factors Risk of business deterioration due to shutdown resulting from inadequate facility maintenance, changes in circumstances surrounding the nuclear fuel cycle business (e.g., front-end business and back-end business), delays in responding to changes in relevant regulations, and injunction lawsuits against nuclear power generation
		《3》 Blackout, etc.	Risk of disruptions to stable supply due to significant deficiencies in facility maintenance, management of supply-demand fluctuations, etc.
Common to all businesses	Strategy	《4》 Delays in responding to rapid changes in the competitive environment	Risk of delays in responding to rapid changes in the competitive energy business environment brought by changes in customer needs and the emergence of competitors
		《5》 Changes in laws, regulations, and regulatory policies	Risk of losing customers due to changes in the business environment, such as institutional design of power system reforms, changes in energy and environmental policies, and tax system reforms
		《6》 Stagnation of innovation	Risk of significantly lowering our reputation among stakeholders due to failure to adapt to the external environment, including political, economic, social, and technological fronts
		《7》 Damage to asset value	Risk that changes in regulations, technological innovations, or other factors may undermine the asset value of each business of the Group
	Strategy / Operation	《8》 Fluctuations in the human capital base	Risk of employee motivation and engagement declining due to the occurrence of work-related casualties, physical or mental illnesses of employees or their families, or a decline in motivation, job satisfaction, or sense of mission Risk where human resources necessary for business continuity will not be secured in terms of both quality and quantity
		《9》 Instability or disruption in the supply chain	Risk of instability or disruption of conventional supply chains due to labor shortages, deteriorating profitability, etc. at suppliers
		《10》 IT governance and information security risks	Risk of delays or impediments in IT and DX promotion due to inadequate strategies and resource allocation, or deficiencies in system development, maintenance, and operation Risk of interference with business or loss of public trust due to ill-preparedness against factors including cyber attacks and information leaks
		《11》 Governance and compliance risks	Risk of loss of public trust due mainly to deficiencies in internal control systems, non-compliance, erroneous financial reporting, and inadequate information disclosure (including the group companies)
	Operation	《12》 Environmental issues (violation of environmental laws and regulations, etc.)	Risk that business activities may impact the surrounding environment or lead to a loss of public trust due to violation of environmental laws and regulations or result in environmental pollution not contrary to laws or regulations
	Hazard / Strategy	《13》 Natural disasters, changes in international situations, etc.	Risk of negative impact exerted on business activities due to delays in responding to economic security (including internal threats) required for disruptions in service supply or changes in international conditions due to natural disasters, armed attacks, spread of infectious diseases, etc.
	Finance	《14》 Market condition / market fluctuation risks	Risk that market fluctuations in JEPX, fuel, and real estate prices, as well as interest and exchange rates may affect business activities

For major risks, we will evaluate the gravity of each from the perspective of probability of occurrence and degree of impact, while determining the actual conditions and characteristics at each business. Countermeasures will then be discussed, followed by evaluation of the gravity again at the end of the fiscal year based on the results of risk countermeasures during the period. This constitutes the PDCA cycle of risk management.

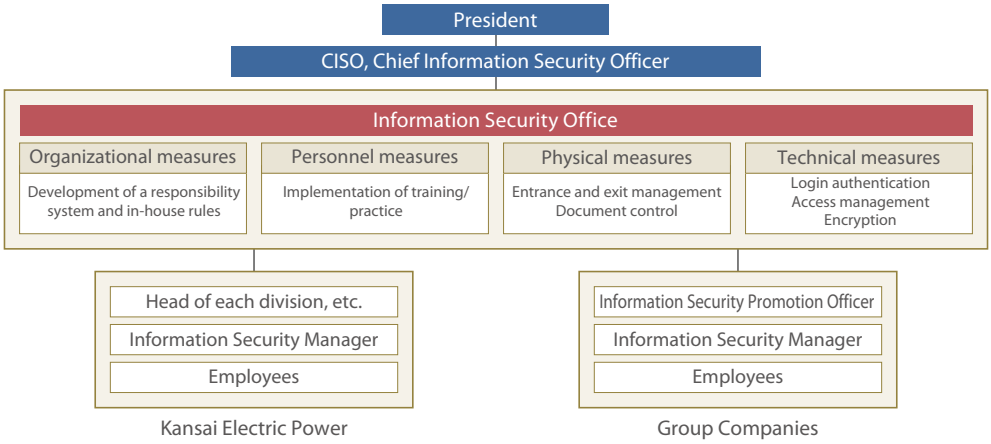
Information security measures

Policy and Concept

With increasing awareness of personal information and accelerating data utilization with widespread digitization, the Act on the Protection of Personal Information imposes more stringent obligations on business operators that handle personal information. The Group believes that the proper protection of personal information is an important responsibility in order to earn the trust of customers and many other people in society, as well as to fulfill our mission as an enterprise. Fully recognizing the importance of personal information the Company and group companies obtain from our customers, etc. that we must handle carefully under principles of respect for the individual, we deal with personal information appropriately in consideration of rights as the right to privacy, in compliance with the Act on the Protection of Personal Information and other guidelines.
With regard to information security, including proper handling of business and personal information, measures on an organizational, personnel, physical and technical level have been implemented. We seek to improve on these measures by incorporating internal and external events as well as reviewing the latest technology and knowledge as appropriate.

System

Responsible director: Makoto Araki [Kansai Electric Power CISO (Executive Vice President)]
Deliberative body: Executive Meeting
Management office: Cyber Security Administration Group, Office of IT Strategy (Information Security Office)



Efforts

The Group works to enhance information security. Our efforts include strengthening physical and technical measures such as entry/exit controls and access controls for information systems. Organizational and personnel measures such as reviewing internal rules, training employees, and training to defend against targeted email attacks are also ongoing.

Participation rate of information security training in FY 2024
1st half 99.5% (7,887 participants in June 2024)
2nd half 99.4% (7,984 participants in December 2024)

Relevant data

	FY 2022	FY 2023 1H	FY 2023 2H	FY 2024 1H	FY 2024 2H
Number of information security training participants	8,411	7,623	8,016	7,887	7,984
Number of major information security incidents*	1	0	0	0	0

* Figures including values representing the Company, Kansai Transmission and Distribution, Inc., and group companies