Introduction   Vision   Material Issues   **Governance**   Data

Board Members   Messages from Outside Directors   Sustainability Promotion Framework   Corporate Governance   Intellectual Property Management
Risk Management and Internal Controls   Compliance

Risk Management and Internal Controls

## KDDI's Approach (Risk Management and Internal Control)

In the ever-changing business environment, the risks that companies face are increasingly diverse and complicated.

We define factors and events that negatively influence the achievement of our business goals as risks and consider enforcing risk management as material business challenge. In order to be sustainable and responsible to society, we promote risk management initiatives throughout the KDDI Group.

KDDI's Risk Management and Internal Control

We have established a system to centralize the management of risks with the Corporate Risk Management Division at the core.

Furthermore, we are promoting risk management throughout the KDDI Group, in order to realize the continuous growth of the entire group. We have appointed 39 Internal Control System Managers within KDDI and 46 at group companies, as well as 5 Internal Control System Directors to oversee their activities. Under their leadership, we introduce and run internal control systems, carrying out risk management activities and run operational quality improvement activities to foster a company culture in which risks are less likely to arise.

▌ Personnel in Charge of Internal Control
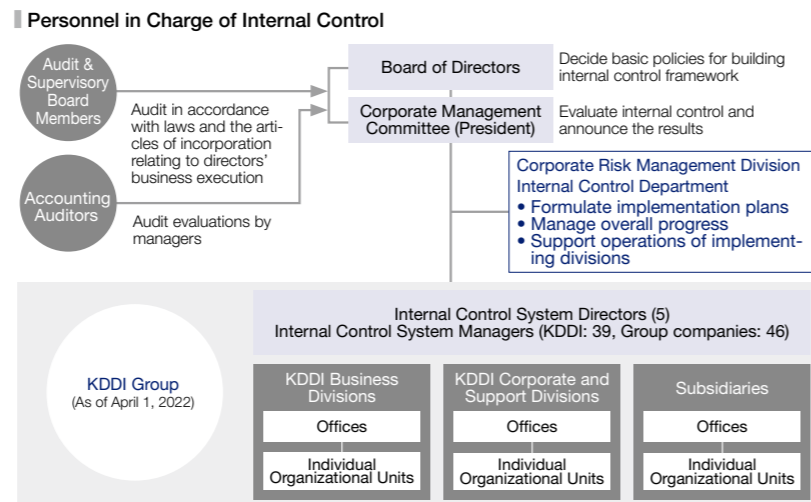
Risk Management Activity Cycle

In order to prevent critical events for the company, we at KDDI consider that it is important to recognize signs of danger and implement preventive measures before the situation worsens. Based on this idea, we follow the PDCA cycle for risk management. We also have an organizational framework for risk management in place to ensure any risks we find will be addressed promptly and appropriately.

Risk Identifying Process

We regularly examine information about risks to identify significant risks that seriously influence corporations, and discuss measures to reduce such risks and their impacts as much as possible in case we face them.

In order to ensure the achievement of our business goals, in FY22.3, we selected 31 significant risks based on issues that manifested in the past and changes in the business environment, and held internal audits centered on risk prediction, the reduction of significant risks and risk approach. The selected significant risks include cyber-attacks, an area that is becoming increasingly complex, global businesses, and issues arising from the expansion of new business fields such as e-commerce, finance and accounting, and energy as a result of the integration of telecommunications and life design, by the previous mid-term management strategy. In order to minimize information security risks, we have also established a common standard applicable group-wide to improve the level of information security across the group.

The status of these significant risks is also reflected on business risks that are revealed in the Securities Report* since it relates to the finance as well.

*For details, please see the Business Risks section of the Securities Report for FY23.3. (Japanese only)

Basic Policy for Constructing an Internal Control System

Based on the provision of Article 362, Paragraph 5 of the Companies Act, we passed the Basic Policy for Constructing an Internal Control System at a meeting of the Board of Directors. In addition, we publicly announce resolutions and our operational status to ensure the fair, transparent and efficient execution of our corporate duties and maintain an effective system for internal controls to raise the company's quality level.

▌ Main Operational Risks

Risk	Competitors, rival technologies and rapid market shifts	Protection of confidentiality of communications and customer privacy (personal and corporate information)	Natural disasters and other unforeseen events	Laws, regulations, and government policies relating to the telecommunications sector	Acquisition of human resources, training and personnel management
Risk background	• The need to provide user support for product defects problems attributable to the rapid expansion of the commerce business • Inability to acquire needed bandwidth we need • Increase in competition due to new high-speed wireless data technology • Possible rise in connection fees with other telecommunications operators • Intensifying competition as a result of changes in the business landscape due to partnerships with other industries, sales packages that include other products (such as telecommunications + power), the emergence of MNOs and MVNOs in the market and other companies expanding their business fields	• Internal privacy breaches • Unauthorized access from external networks	• Natural disasters, such as earthquakes, tsunamis, typhoons, or floods, as well as secondary damage from the spread of toxic substances caused by natural disasters • Worldwide spread of an infectious disease (pandemic) • War, terrorism, accidents, or other unforeseen events • Power brownouts or blackouts • Computer viruses or other forms of cyber-attack and hacking • Operation system hardware or software failures • Flaws in communication equipment and services	• Revisions to the calculation formula for inter-operator connection fees and / or accounting methods • Revisions to designated telecommunications facilities system and / or the regulations on prohibited activities • Revisions to the universal service systems • The emergence of MNOs and MVNOs in the mobile communication market • Revisions to the frequency allocation system and / or spectrum user fee system • Changes in rules regarding electricity retail and financial business, etc. • Changes in rules regarding the usage of personal data, etc.	• Rise in human resources investment costs in the future
Potential impact on KDDI	• Negative impacts on the financial position and operations of the KDDI Group	• Could seriously damage the brand image of the KDDI Group. In addition to a possible loss of customer trust, we could also be forced to pay substantial compensation or surcharge • In the future, we may face higher costs to develop the framework necessary to protect the confidentiality of communications and customer privacy • Could have a negative impact on the financial position and / or earnings performance of the KDDI Group	• Service outages or interruptions as a result of large-scale natural disasters or accidents caused by climate change, etc. • Loss of opportunities to offer products and services due to service outages as a result of failures in network systems or communication equipment, substantial billing errors, closing of distributors, or suspension of distribution and reputational damages through media such as SNS could damage the brand image of the KDDI Group and lead to loss of customer trust and decreased customer satisfaction, which could have a negative impact on the earnings performance • The Company's future business activities and earnings performance could be affected by customers' lost opportunities to use au Shops due to shortened store operating hours, reduced mobile data usage due to increased Wi-Fi usage at home, and the various influences on our life design business and solution services for corporate customers	• The KDDI Group's earnings performance could be negatively impacted by the revision or abolishment of laws and regulations or formulation of government policies relating to telecommunications and finance business • The KDDI Group's earnings performance could be negatively impacted if the company's competitive advantage is relatively diminished as a result of competition	• If we are unable to handle matters appropriately in the future, the KDDI Group's brand image could be damaged, leading to loss of customer trust and a negative impact on our earnings performance
KDDI's response	• The creation of new value and the achievement of sustainable growth in the 5G / IoT era domestically and globally with a business strategy that focuses on the previous mid-term management strategy "integration of telecommunications and life design," which centers on telecommunications and expands peripheral businesses	• Establishment of the KDDI Code of Business Conduct, KDDI Security Policy, and KDDI Privacy Policy • Establishment of the Business Ethics Committee • Reinforcement of various technical, organizational and human safety management measures • Educating all employees on the protection of confidentiality of communications and customer privacy • Working with our external partners, particularly with our retail network of au Shops, to strengthen management through the improvement of shop operations, monitoring and training • Establishing Information Security Committee • Acquiring external authentication (ISMS) in the whole company • 24 / 7 monitoring of external attacks by specialists	• Initiatives to improve reliability of our network and prevent service outages by implementing Business Continuity Planning • Establishing a disaster response headquarters as early as possible in the event of an emergency or disaster • Contract procedures available online 24 hours a day • Initiatives to ensure the safety of customers and employees	• Taking appropriate actions based on laws, regulations and government policies • Advocating measures for fair competition with other telecommunications operators through various deliberation councils and study sessions as well as the public comment system of the Japan's Ministry of Internal Affairs and Communications	• Working together across the entire company to support personnel training and career development to keep up with technological innovations • Appropriate personnel management and the promotion of work style reforms based on the law

Initiatives in Response to the Internal Control Reporting System (J-SOX)

In response to the internal control reporting system based on the Financial Instruments and Exchange Law implemented in FY09.3, we conducted evaluations of the internal controls at KDDI and 10 major group subsidiaries (totaling 11 companies) in and outside Japan to ensure reliability of our financial reporting. The results of these evaluations were compiled in an internal control report, which was submitted to Japan's Prime Minister in June 2022, as well as disclosed to investors.

Activities to Enhance Operational Quality

In conjunction with the response to the internal control reporting system, we established an Internal Control Department that promotes initiatives for improving the overall operational quality of the whole Company, and Internal Control System Managers in each department facilitate initiatives that enhance the efficiency and standardization of operations to do so. Business improvement projects through this activity are added to a database, enabling all employees to utilize activities to enhance operational quality in their own departments.

Furthermore, to further raise each employee's awareness and motivation regarding the quality of operations, we have introduced the Operational Quality Improvement Prize to recognize excellent and ambitious initiatives. In addition, we have started working on the introduction of robotic process automation (RPA) across the Company as a way of improving operational quality, productivity, and efficiency at the same time, starting with the preparation of the RPA system environment and education programs.

Activities to Enhance Operational Quality
• e-learning training
• Sharing messages from executives and good examples of initiatives in e-mail newsletters and internal magazines
• Implementation of Operational Quality Improvement Prize (Once a year)