Risk Management and Internal Controls

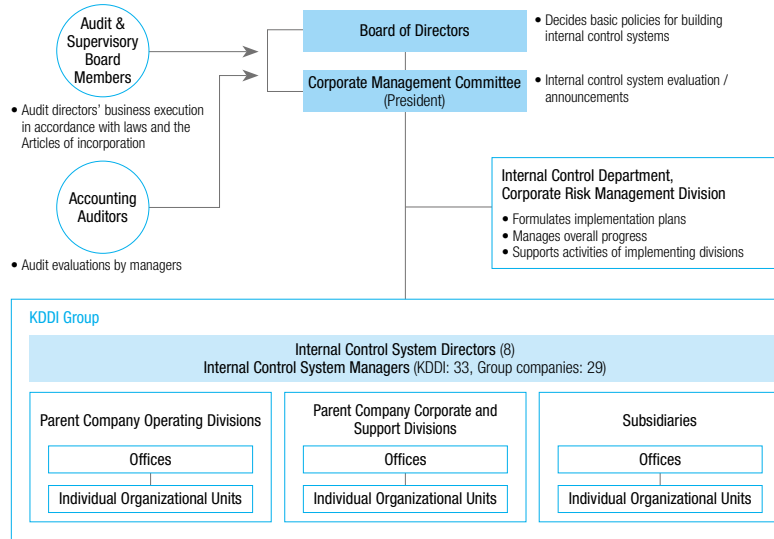## KDDI's Risk Management and Internal Control Promotion

KDDI has established a system to centralize the management of risks, which it defines as factors that have the potential to block the achievement of management objectives. The Risk Management Division is the core of this system. In addition, KDDI is working to promote risk management across the entire Group, including KDDI as well as its subsidiaries, in order to achieve continuous Group-wide growth.

KDDI has appointed 33 Internal Control System Managers and Group companies have appointed 29, as well as 8 Internal Control System Directors to oversee their activities. This structure forms the basis for our internal control system and its operation as well as our risk management activities. We also promote operational quality enhancement activities to realize a corporate constitution that prevents risks from materializing.

In FY2015, to realize our management objectives with certainty, KDDI designated 32 items as significant risks, reflecting on issues that have come to the fore in the past and changes in our operating environment, such as the provision of high quality networks, homogenization of products and services with rival companies, and expansion into new business domains. KDDI worked to foresee risk, engaged in activities to reduce significant risks, and conducted internal audits based on a risk approach.

Furthermore, we are undertaking Companywide initiatives to improve the quality of our operations, thereby cultivating a corporate culture that prevents risks from materializing.

Internal Control Systems

Board of Directors
- Decides basic policies for building internal control systems

Corporate Management Committee (President)
- Internal control system evaluation / announcements

Audit & Supervisory Board Members
- Audit directors' business execution in accordance with laws and the Articles of incorporation

Accounting Auditors
- Audit evaluations by managers

Internal Control Department, Corporate Risk Management Division
- Formulates implementation plans
- Manages overall progress
- Supports activities of implementing divisions

KDDI Group

Internal Control System Directors (8)
Internal Control System Managers (KDDI: 33, Group companies: 29)

Parent Company Operating Divisions	Parent Company Corporate and Support Divisions	Subsidiaries
Offices	Offices	Offices
Individual Organizational Units	Individual Organizational Units	Individual Organizational Units

Efforts to Improve Risk Response

KDDI understands the importance of establishing a business culture that recognizes risk and constantly improves operations to reduce risk, along with the need to secure a system that takes an appropriate response when risk is discovered. As a result, all divisions and their directors work in cooperation with the Risk Management Division, which regularly identifies and uniformly manages risk information. The KDDI Group's risks are managed appropriately in accordance with internal regulations, and efforts are made to achieve business objectives fairly and efficiently. These risks are prioritized according to their potential for serious and long-term effects on the company, and KDDI examines and establishes measures to minimize the risk to business operations as much as possible.

Also, in addition to establishing an internal reporting system, KDDI engages in a variety of company-wide efforts to improve the ability to respond to risks, through activities such as disaster-preparedness drills, risk management training, and risk-related information sharing.

Risk Management and Internal Controls

Policy

Basic Policy for Constructing an Internal Control System

Based on the provisions of Article 362, Paragraph 5 of the Companies Act, KDDI passed the Basic Policy for Constructing an Internal Control System at a meeting of the Board of Directors and issued a public announcement. KDDI aims to ensure fair, transparent and efficient execution of its corporate duties and to maintain an effective system for internal controls.

The contents of the Basic Policy for Constructing an Internal Control System are provided below.

1 Corporate Governance

(1) The Board of Directors

The Board of Directors is composed of both internal and external Directors, who determine important legal matters as stipulated by laws and ordinances based on the Board's regulations and Agenda standards. In addition, the Board oversees the competent execution of business duties by the Directors themselves. Information pertaining to the execution of business duties by the Directors must be stored and managed appropriately in accordance with internal regulations.

(2) System for executing business duties

[1] The Executive Officers' System aims to clarify both the delegation of authority and responsibility system, as well as ensure that tasks are executed effectively and efficiently.

[2] The Corporate Management Committee, which is composed of Directors and Executive Officers, shall discuss and determine important matters pertaining to the execution of tasks, as well as discussing and determining the Board's Agenda items, based on the Corporate Management Committee regulations.

(3) System for ensuring the effective execution of business duties by Auditors

[1] Auditors shall attend the Meetings of the Board of Directors and, additionally, steps shall be taken to allow them to attend the principle internal meetings of the company.

[2] The Board of Directors, Directors of subsidiaries, and Internal Auditing Division aim to collaborate by providing timely, appropriate information necessary for executing the business duties of the Auditors, as well as by exchanging opinions and ideas.

[3] The Auditing Office was established to support the business duties of the Auditors; in order to ensure appropriate staffing levels due consideration shall be given to aptitude, the number of personnel required, etc., and the opinion of the Auditors.

[4] Steps shall be taken to ensure that a person who has reported to the Auditors shall not suffer any consequences on account of having made such report.

[5] The Auditors shall be assured of the costs required by them to carry out their duties effectively.

2 Compliance

(1) All executives and employees should continuously maintain high ethical standards in accordance with the basic principles set forth in the 'KDDI Action Guideline,' which should be complied with, and aim to execute their business duties properly.

(2) Firm measures should be taken against antisocial forces, and efforts should be made to sever all such relationships.

(3) Each KDDI Group company shall make efforts to promptly identify and resolve any serious violation of laws and ordinances or other compliance-related matters or incidents, at KDDI Group company meetings pertaining to business ethics.

(4) KDDI shall aim to appropriately operate a compliance-related internal reporting system established both internally and externally to the company.

(5) KDDI shall strive to improve the understanding and awareness of compliance through both internal and external training and enhancement activities.

3 Risk management for achieving business goals fairly and efficiently

(1) KDDI shall conduct business risk analyses, stringently prioritize business activities and formulate appropriate business strategies and business plans at meetings participated in by Directors concerning business strategy, with the objective of continuous growth for the KDDI Group. To achieve this, business risk should be monitored monthly at meetings pertaining to performance management, and this performance should be managed thoroughly.

(2) In each Division a person shall be appointed as the person responsible for internal control, and this person shall autonomously promote the following initiatives so that business objectives may be achieved fairly and efficiently.

[1] All Divisions and their Directors shall work in cooperation with the Risk Management Division, which regularly identifies and uniformly manages risk information. The KDDI Group's risks shall be managed appropriately and in accordance with internal regulations, and efforts shall be made to achieve business objectives fairly and efficiently.

[2] KDDI shall examine measures for minimizing the risk of business interruptions as much as possible in order to respond to events which could have serious and long-term effects on corporate business.

[3] In accordance with the internal control reporting system based on the Financial Instruments and Exchange Act, KDDI shall implement documentation, assessment and improvement of the state of company-wide internal control and of important

Risk Management and Internal Controls

business processes on a consolidated basis, with the aim of further improving the reliability of financial reporting.

[4] KDDI shall aim to maintain and enhance the systems necessary to improve the quality of business duties of the KDDI Group, including enhancement of the effectiveness and efficiency of business duties and appropriate acquisition, safekeeping and disposal of assets.

(3) In its role as a telecommunications carrier, KDDI shall pursue the following initiatives.

[1] Protecting the privacy of communications

Protecting the privacy of communications is at the very root of the KDDI Group's corporate management, and the Group will abide by this.

[2] Information Security

KDDI aims to manage the company's total information assets, including preventing leaks of customer information and cyber-terrorism of networks for telecommunications services, by formulating measures at meetings pertaining to information security to ensure this security in cooperation with the Directors.

[3] Recovering networks and services in times of disaster

In order to minimize as much as possible the risk of a termination or interruption to telecommunications services in the event that a major accident, obstruction or large-scale disaster occurs, a Business Continuity Plan (BCP) shall be formulated and measures shall be implemented to improve network reliability and prevent the halting of services. In order to facilitate a prompt recovery in times of emergency or disaster, a Disaster Response Headquarters shall be established as expeditiously as possible.

4 Initiatives relating to working together with stakeholders

(1) The whole company shall make efforts to gain support and trust for all KDDI Group activities, improve customer satisfaction, and

strengthen and expand the company's customer base.

[1] By regarding all stakeholders as customers, and through the prompt and appropriate response to customer needs and complaints, all executives and employees shall engage in TCS (Total Customer Satisfaction) activities that aim to improve the level of customer satisfaction. To promote these activities, efforts shall also be made at meetings pertaining to TCS to evaluate and improve TCS activities.

[2] In addition to providing customers with safe, secure, high-quality products and services in compliance with the pertinent laws and regulations, information about products and services should be provided in an easy-to-understand format and indicated appropriately, so that customers can select and use the most appropriate product and/or service.

(2) In order to gain the understanding and trust of all stakeholders, transparency of KDDI Group management shall be ensured, and efforts shall be made to further enhance the PR and IR activities of the KDDI Group.

(3) The KDDI Group's business risk shall be fairly identified and disclosed in a timely and appropriate manner at meetings pertaining to information disclosure. In addition, Integrated Report (Detailed ESG Version) shall be created and disclosed, centering on those departments promoting CSR, for matters pertaining to the KDDI Group's social responsibilities, including its environmental efforts and contributions to society.

5 Systems for ensuring business suitability of corporate groups

(1) Each member company of the KDDI Group shall appoint a person responsible for internal control in order to ensure appropriate business operations across the entire KDDI Group.

(2) On the basis of the management regulations for subsidiaries, collaboration with subsidiaries shall be maintained through the

establishment of a system through which subsidiaries submit appropriate, timely reports.

(3) Risk management shall be handled appropriately in the subsidiaries so as to achieve business goals fairly and efficiently.

(4) In addition to working, through KDDI Group company meetings pertaining to the business ethics, to promptly identify and resolve any serious violation of laws and ordinances by a subsidiary or any other compliance-related matter or incident, all subsidiary personnel shall at all times maintain high ethical standards in accordance with the KDDI Action Guideline, and ensure a system is in place whereby business duties are carried out appropriately.

6 Internal Audits

Internal audits are conducted for all aspects of business of the KDDI Group, and the suitability and effectiveness of the Internal Control system is verified regularly. The results of internal audits are reported to the President with added suggestions for points that can be improved or revised, and a report is also made to the Auditor.

Activity and Results

Initiatives in Response to the Internal Control Reporting System

In response to the Internal control reporting system based on the Financial Instruments and Exchange Law implemented in FY2008, KDDI established internal control systems at the Company and major Group subsidiaries in Japan and overseas, and conducted evaluations of its internal controls to ensure reliability in its financial reporting. The results of these evaluations were compiled in an internal controls report, which was submitted to the Japanese Prime Minister in June 2016, as well as disclosed to investors.

Risk Management and Internal Controls

Activity and Results

Protecting Intellectual Property

KDDI's commitment to creating and protecting intellectual property and respecting the intellectual property rights of others is defined in the basic policies of the KDDI Code of Business Conduct.

Furthermore, it has formulated intellectual property handling regulations to ensure the proper management and usage of KDDI's inventions, ideas, designs, trademarks, and other industrial property; software and other copyrighted materials; and technologies, expertise, and other rights protected under the Unfair Competition Prevention Act.

As part of its efforts to provide customers with high-speed, high-quality, safe and secure communication services, KDDI conducts research and development of technology to increase communication speed, such as LTE and 5G, as well as security technology that provides privacy protection. As a result of these activities, KDDI holds approximately 2,000 patents in Japan and 250 patents overseas, as of the end of March in 2016. Moving forward, KDDI will continue to bolster its intellectual property assets and strengthen its competitiveness both in Japan and overseas.

In addition, KDDI conducts educational activities every year through group training and e-learning classes, to provide employees with a deeper understanding of the importance of intellectual property, as well as the risks of infringement and its prevention.
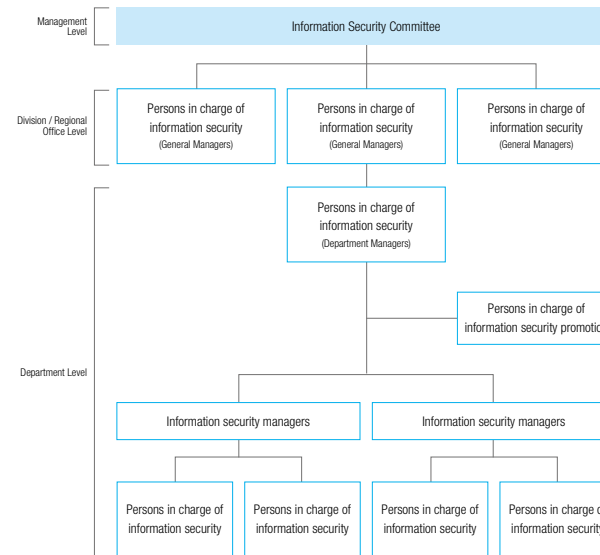
System

Information Security Management System

KDDI has established an Information Security Committee composed of management-level employees, along with the heads of the sales, technology, and corporate administrative divisions. This committee is part of a structure that carefully recognizes the status of information security controls for the entire company, and when necessary readily implements Group-wide measures to enhance information security.

Security Management Structure

Management Level — Information Security Committee

Division / Regional Office Level — Persons in charge of information security (General Managers)

Persons in charge of information security (Department Managers)

Persons in charge of information security promotion

Department Level — Information security managers

Persons in charge of information security

Policy

KDDI's Security Policy

KDDI recognizes the appropriate management of information as a topmost management priority. Accordingly, we have formulated the Security Policy as our basic policy on information security. To earn the trust of customers and other stakeholders, we publicize this policy both inside and outside the Company and declare our observance to it, consistently taking appropriate defensive action to counter the risk of information leaks.

Security Policy
Link ▶ Website

Policy

KDDI's Privacy Policy

KDDI realizes the importance of personal information. To ensure the thorough protection of such information, KDDI conforms with the Telecommunications Business Law, legislation concerning the protection of personal information, industry-specific guidelines such as those related to the protection of personal information in the telecommunications business, and other laws. We also publicize and declare adherence to our basic policy in this area, the Privacy Policy.

Privacy Policy
Link ▶ Website

System

Strengthening Information Security

KDDI is making serious efforts to strengthen information security, in order to prevent the leakage of information entrusted by numerous individual and corporate customers, including approximately 45.91 million au customers.

Risk Management and Internal Controls

KDDI has established and administers an Information Security Committee composed of management-level employees, along with the heads of the sales, technology, and corporate administrative divisions. This committee is part of a structure that carefully recognizes the status of information security controls for the entire Company, and readily implements measures to enhance information security at KDDI itself and throughout the Group.

In April 2009, we acquired information security management system (ISMS) certification* (ISO/IEC 27001) for the entire company. Since then, we have continued to implement measures to improve information security centered on the maintenance of these systems. In FY2012, we formulated regulations for KDDI Group companies based on the KDDI Group Information Security Standards that we formulated in FY2011. Since FY2013 we have continued working to strengthen information security and governance at KDDI Group companies through the appropriate execution and timely inspection of Group company regulations and application of a PDCA cycle.

* This is a third-party certification system for information security systems. It was established with the goal of contributing to widespread improvements in information security and encouraging companies to target levels of information security that can be trusted around the world.

ISMS Certification at KDDI

Registration Number	Organization	Initial Registration
IS 95253	KDDI CORPORATION [1]	June 7, 2005
IS 76406	KDDI CORPORATION (Operations Division) [2]	July 4, 2003
IS 85329	KDDI CORPORATION (Information Systems Division)	September 28, 2004

[1] Includes corporate, technology and sales, and customer support divisions, as well as KDDI KYOSAIKAI (now, KDDI Group Welfare Association), KDDI Health Insurance Union, KDDI Pension Fund, KDDI Research Institute, Inc. and KDDI MATOMETE OFFICE CORPORATION

[2] Includes Japan Telecommunication Engineering Service Co., Ltd.

System

Responding to Incidents Involving Information Leaks via Social Media

The expanding use of social media has prompted a spate of incidents in which corporate trust has been damaged or individual privacy compromised over the Internet. KDDI has addressed this situation by formulating and disseminating thoroughly rules that all executives and employees must follow when using social media.

System

Preventing Information Leaks Due to Emailing Errors

Email has supplanted the telephone as an essential two-way communication tool for business. However, a major issue when using email is preventing information leaks caused by sending emails to the wrong address, attaching the wrong documents, or other mailing errors.

To resolve these issues, KDDI has introduced mechanisms for preventing emailing errors, such as prevention of automatic mail forwarding, automatic encoding of attached files when emails are sent outside the company, temporary delays before sending, and mandatory bcc of addresses (prevention of leaking of email addresses). In these ways, we are bolstering activities to prevent information leaks accompanying emailing errors.

System

Activities to Enhance Operational Quality

KDDI considers its initiatives in response to the internal control reporting system to be part of its ongoing effort to improve overall corporate quality. The Internal Control Department, established as part of the response to this system, acts as the managing authority for the entire Company's internal control efforts, and Internal Control System Managers take the role of facilitators in each division and work to improve overall corporate quality by enhancing operational efficiency and providing standardization, while at the same time raising the quality of operations and the degree of added value.

To increase individual divisions' motivation to improve operating processes, KDDI has introduced the Operational Quality Improvement Prize to recognize excellent and motivational improvements. In addition, KDDI is conducting operational quality enhancement activities aimed at boosting the motivation of each employee to make individual improvements that enhance the quality of KDDI's operations and lead to stronger business results. Through these activities, the business process improvements made by all employees are implemented one by one on a continuous basis. This encourages independent action to become firmly rooted in our corporate culture, while strengthening our efforts to focus on the customer's perspective.

Infusion

Spreading Operational Quality Enhancement within the Company

We are undertaking a number of measures to ensure that this initiative gets through to all employees, enhancing their understanding of internal control and making the activities a permanent fixture. For example, the sharing of executive messages and positive case studies through a regular email magazine and our internal newsletter, and the conducting of e-learning classes.