CORPORATE ETHICS

GRI 2-23

Corporate ethics issues in Kazakhtelecom JSC are governed by the Code of Business Conduct and the Corporate Governance Code. The Code of Business Conduct and the Corporate Governance Code are public documents and are freely distributed by the Company to employees, shareholders, customers, partners, and other stakeholders.

The Code of Business Ethics of Kazakhtelecom JSC was developed in accordance with the legislation of the Republic of Kazakhstan and takes into account the requirements of the International Labour Organization, as well as the Company's Charter, Corporate Governance Code, and a number of other internal documents of Kazakhtelecom JSC.

The provisions of the Code of Business Ethics and the Corporate Governance Code are mandatory for all employees and officers of the Company.

All officers and employees are required to confirm in writing that they have read and understood the Code of Business Ethics. In addition, the Company regularly conducts training sessions for officers and employees to ensure awareness of the Code of Business Ethics, the role of the Ombudsperson, and the availability of the whistleblowing system for reporting suspected violations. In 2024, a total of 12,104 employees of the Company completed training on the Code of Business Ethics.

The Company's key principles of business ethics include:

- Compliance with legal requirements;
- Fairness;
- Integrity;
- Transparency;
- Accountability;
- Competence and professionalism;
- Trust;
- Meritocracy.

The Ombudsperson is responsible for ensuring adherence to ethical principles and resolving social and labor-related conflicts. The Ombudsperson is an employee of the Company appointed by the Board of Directors to support conflict prevention and resolution in labor relations, protect the rights and legitimate interests of employees, promote corporate values, and uphold the principles of business ethics.

The Code of Business Conduct of Kazakhtelecom JSC is available on the Company's website telecom.kz.

RISK MANAGEMENT AND INTERNAL CONTROLS

The Corporate Risk Management and Internal Control System (CRMS and IC) is aimed at providing reasonable assurance of achieving the goals set by the governing body of Kazakhtelecom JSC.

In today's environment, emerging risks in the telecommunications sector include cybersecurity threats, changes in legislation and regulatory frameworks, as well as technological challenges such as the deployment of 5G and the Internet of Things (IoT). The increasing number of cyberattacks on communication networks poses risks of confidential data breaches, service disruptions, and significant implications for both business operations and society at large.

As the largest telecommunications operator in Kazakhstan, Kazakhtelecom JSC plays a key role in advancing telecommunications infrastructure and ensuring the security of communications across the country. The Company actively adopts modern technologies and strives to enhance the cybersecurity of its networks to protect customer data and ensure the uninterrupted delivery of communication services. These efforts are supported by the functioning of the Corporate Risk Management and Internal Control System CRMS and IC) at Kazakhtelecom JSC, which is designed to safeguard assets, improve business processes, enhance operational efficiency, and ensure compliance with applicable legal requirements.

The timely identification of non-conformities and inefficiencies, the analysis and forecasting of potential scenarios, and the development of preventive and mitigating measures make a significant contribution to the achievement of the Company's operational and strategic objectives.

MODEL OF RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM

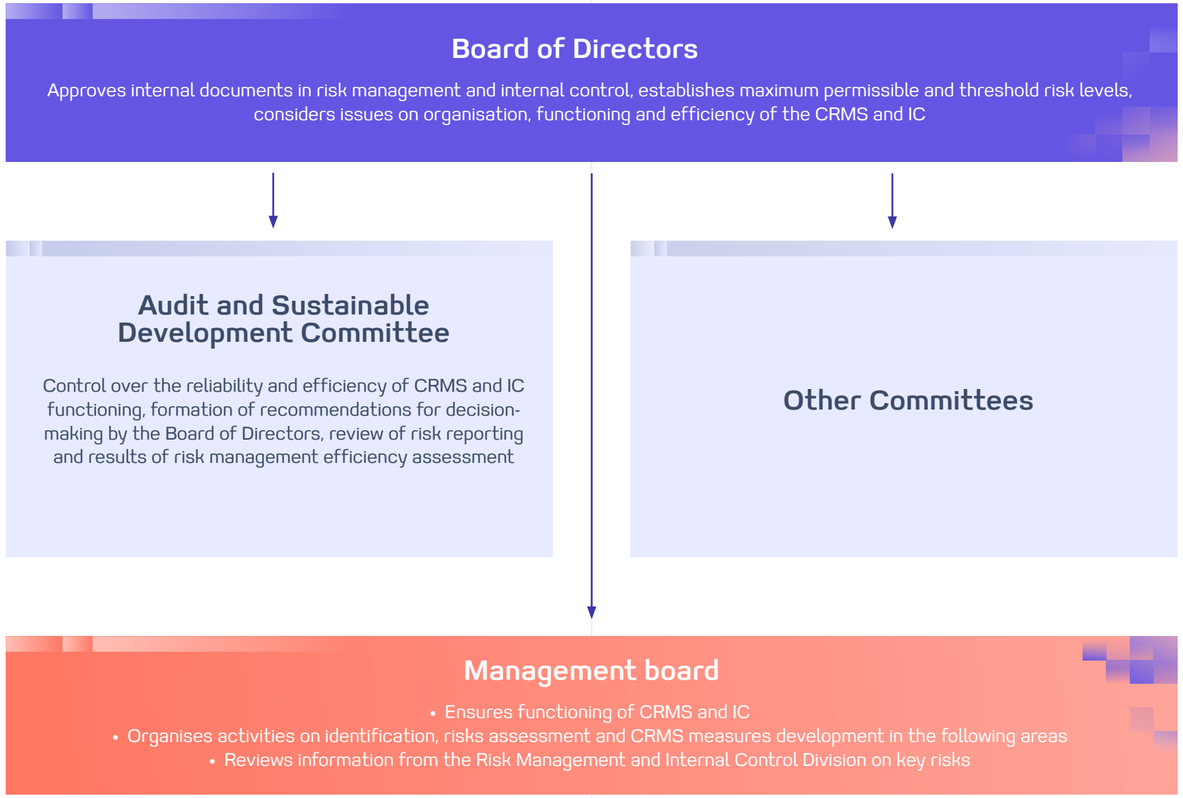
The Company's CRMS and IC functioning model involves all levels of corporate governance in the timely identification and management of risks and non-conformities, and includes building CRMS and IC components at the strategic and tactical management levels as well as ensuring independent assessment and oversight of its functioning.

MAIN TASKS AIMED AT ACHIEVING THE OBJECTIVES OF THE INTERNAL CONTROL SYSTEM

1. Forming and updating the main areas of development of the Internal Control System (ICS) in accordance with the Company's needs and the stakeholders' requirements
2. Risk assessment of business processes, development, implementation and execution of control procedures, including unified methodological support for the organisation and effective functioning of ICS in the Company
3. Identification of deficiencies in existing control procedures, development and implementation of measures to eliminate them, typification and regulation of control procedures
4. Development and implementation of mechanisms for interaction and exchange of information on internal control between CRMS and IC subjects to build a preventive system for identifying operational risks, including through the information systems use

As part of the above tasks, the Company works to identify business process risks, develop and implement control procedures which helps to improve the efficiency and manageability of business processes, ensure the reliability of financial reporting, compliance with legal requirements and local regulatory documents of the Company.

ORGANISATIONAL STRUCTURE OF THE CORPORATE RISK MANAGEMENT SYSTEM



ORGANISATIONAL STRUCTURE OF THE CORPORATE RISK MANAGEMENT SYSTEM

FIRST LINE Operational risk management	SECOND LINE Control and monitoring function	THIRD LINE Independent assessment
Risk supervisors, risk owners, business process and control owners • Identifying, assessing, managing and minimising risks • Ensuring an effective internal control system	**Controlling divisions, Risk Management and Internal Controls Department** • Coordination and improvement of the risk management and internal control process • Monitoring and control of the risk management and internal control system • Compliance with internal corporate requirements • Compliance with legal requirements	**Internal audit** • Independent assessment of the effectiveness of risk management, internal control and corporate governance systems

The Company recognises that risk management is effective only when every employee is in the process. Therefore, we are constantly developing a risk-oriented culture with the following key aspects:

TONE ON TOP

The Company's management sets an example for employees in discussing, identifying and assessing risks, and is actively involved in risk management.

CULTURAL SPECTRUM

Timely provision of risk information is encouraged. Acceptance of risks is allowed if they are not critical but may contribute to business development. The risks themselves are viewed not only as a potentially negative event, but also as an opportunity to improve the Company's processes.

INVOLVEMENT

Risk management training is organised for employees, accessible guidance materials are developed, and communication and support channels are organised.

INTERNAL CONTROLS SYSTEM

The Company has developed and regularly updates internal regulatory documents that define the procedures and principles governing the internal control system, including the Internal Control System Policy and the Internal Control System Management Rules. The updated documentation outlines the following:

- The objectives and principles for building the internal control system;
- The allocation of responsibilities among internal control system participants;
- The main steps and procedures of the internal control process, including responsibilities and timelines for implementation, enhancement, and diagnostics;
- The procedure for updating business process descriptions within the internal control system;
- The process for diagnosing (assessing the effectiveness of) the internal control system and preparing and submitting reports on its current status, including the identification of weaknesses in the internal control system over financial reporting;
- The conduct of independent assessments of the internal control system over financial reporting and its components by the Company's internal audit function.

The Company's internal control system is developed in accordance with recommendations from leading international risk management and internal control practices, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO), TMForum, and ISO standards. The system is based on the "three lines of defense" model.

Responsibility for the system's operation is allocated in line with this model as follows:

FIRST LINE OF DEFENSE

Management (process owners) bear primary responsibility for managing risks associated with day-to-day operations. This line is also responsible for developing, implementing, and operating control mechanisms and monitoring their performance.

SECOND LINE OF DEFENSE

Identifies emerging risks in the Company's daily operations and ensures compliance with regulatory requirements and internal policies. It develops supporting policies, documentation, tools, and technologies.

THIRD LINE OF DEFENSE

Assesses the effectiveness of the internal control system (ICS), reports to the Management Board and the Audit Committee, and provides audit assurance to regulators and external auditors, demonstrating the effectiveness of the control environment and framework.

At Kazakhtelecom JSC, a formalized internal control system over the financial reporting process has been established. The key stages in building and maintaining this system include:

- Describing key business processes involved in financial reporting;
- Identifying and assessing risks at the business process level that could affect the reliability of reporting, and delineating responsibilities for managing these risks;
- Describing, assessing, and implementing control procedures aimed at mitigating process-level risks;
- Describing, assessing, and implementing entity-level control procedures, along with assigning responsibility for their execution;
- Describing, assessing, and implementing general IT controls, and assigning responsibilities accordingly;
- Ensuring timely communication of relevant information to stakeholders.

INTEGRATION OF RISK MANAGEMENT WITH THE COMPANY'S CROSS-FUNCTIONAL PROCESSES

Interrelation of risk management with strategic planning, budgeting, implementation of investment projects and products and other processes:

1 Strategic planning

When developing strategic plans, risks affecting the achievement of strategic goals are identified and analysed.

2 Budgeting

Analysing and accounting for risks associated with failure to achieve key financial KPIs.

3 Implementation of investment projects and products

Analysis and accounting of project and product risks associated with failure to achieve NPV and other indicators, followed by the formation of measures to mitigate risks.

4 Training

Professional development programmes are regularly held for employees involved in risk management. The training course On Risk Management and Internal Controls is available to all employees of the Company.

RISK MANAGEMENT IN 2024

On an annual basis, the Company conducts a risk identification process, the results of which are reflected in the Risk Register and Risk Map, both approved by the Board of Directors. The Risk Register includes risks that may impact the achievement of the Company's long-term strategic objectives and key performance indicators of the Development Plan.

According to the Risk Register and Risk Map as of the end of 2024, the Company has identified 24 risks:

:

The risk map of Kazakhtelecom JSC, developed in accordance with the Risk Register, includes 24 risks that take into account the probability of occurrence and the magnitude of impact. The development of the risk map allows the Company to:

- Identify key risks and develop action plans for their effective management;
- Prioritize risks and allocate financial resources optimally.

Environmental/Climate Risk Factors

The Company's Risk Register includes an "Environmental/Climate Risk," which comprises the following factors:

- Low fuel quality, malfunctioning vehicles and boiler equipment;
- Non-compliance with environmental protection legislation and sanitary regulations, as well as limited employee awareness;
- Breaches in waste and wastewater management requirements;
- Lack of a dedicated structural unit responsible for environmental issues;
- Accumulation of mercury-containing lamps, vehicle tyres and other materials that are not being disposed of;
- Insufficient funding for proper disposal;
- Absence of employee training on environmental matters.

Identified risks in the Register are categorized as follows:

- Financial risks – related to capital structure, market volatility, liquidity, credit risks, and fluctuations in foreign exchange and interest rates;
- Legal risks – losses due to non-compliance with the laws of the Republic of Kazakhstan or other countries;
- Operational risks – losses caused by errors in internal processes, employee actions, information systems, occupational safety, or external factors;
- Strategic risks – losses arising from strategic missteps, changes in the political environment, sectoral downturns, new products, investments, or mergers and acquisitions.
  The corporate register includes 7 strategic risks, of which 5 are in the key risk zone:
  - Customer churn growth;
  - Decline in Kazakhtelecom Group's market share in the telecommunications sector;
  - Project-related risks;
  - Regulatory risk;
  - Risk of losing radio frequency spectrum (RFS).

Action plans have been developed for each of the key risks.

The continuous development and enhancement of the Company's Internal Control and Risk Management System (ICRMS) enables it to promptly adapt to changes in both external conditions and internal business processes, thereby improving operational efficiency and contributing to shareholder value growth. In accordance with the updated Rules for Risk Identification, Assessment and Monitoring at Kazakhtelecom JSC, threshold values and colour coding of the risk map were revised to more accurately reflect the actual risk profile.

In addition, in 2024 the Risk Management Department was placed under the supervision of the Managing Director for Financial Control and Risk, along with the Financial Control Department. As a result, the internal audit and inspection procedures will be updated to place greater emphasis on risk and internal controls.

KEY RISKS OF 2024

The Risk and Internal Control Management Department conducts regular monitoring of changes in key risks and oversees the implementation of measures aimed at their mitigation. The results of this monitoring are reflected in risk and internal control management reports, which are submitted quarterly for review by the Company's Board of Directors.

As part of a proactive approach, the Company implements measures to manage key risks in order to minimise their impact on the achievement of strategic objectives:

KEY RISKS AND MITIGATION MEASURES:

Key risks	Measures taken by the Company to mitigate these risks
Physical Asset Security	› Ensuring security and technical protection systems for Company facilities; › Implementation of the 2024 Fire Safety Business Plan.
Decline in Kazakhtelecom Group's Market Share in the Telecommunications Sector	› Expansion of the E-Kassa ecosystem – including the core cashier platform and mobile application; › Introduction of new services and products to the OFD personal account.
Risk of Loss of Radio Frequency Spectrum (RFS)	› Implementation of measures to preserve unused frequencies.
Deterioration in Financial Stability	› Increased EBITDA revenue targets; › Optimised EBITDA expenditure plans.
Legal Risk	› Formalisation of property rights for unregistered cable duct sections and land plots, and extension of property rights for assets with expired titles; › Development of a regulatory document database titled "Enforcement Proceedings."
Regulatory Risk	› Approval of a roadmap to ensure 100% coverage of fixed telephony with SORM (System for Operative Investigative Activities) tools; › Deployment of SORM functionality across data transmission networks in 10 cities; › Enabling SORM functionality for FWA (Fixed Wireless Access) service.
Fraud Risk	› Prevention and suppression of fraudulent practices among Company employees; › Inspections conducted across the Head Office and Company branches.

KEY RISKS AND MITIGATION MEASURES

Key risks	Measures taken by the Company to mitigate these risks
Quality Risk	› Implementation of the "SAPA+" project to enhance Wi-Fi internet connectivity for Kazakhtelecom clients; › Implementation of the "TAZARTU" project for transitioning copper infrastructure to fibre-optic networks.
Human Resources Risk	› Implementation of the Comprehensive Action Plan to Ensure Social Stability within the Kazakhtelecom Group; › Execution of the 2024 Occupational Health and Safety Action Plan.
Information Security Breach	› Implementation of the "Information Security Protection Modernisation" project; › Awareness-raising activities conducted for employees on information security rules and requirements.

EMERGING RISKS AND OPPORTUNITIES

To ensure preventive risk management measures, the following emerging risks have been identified. These risks are not yet reflected on the risk map, but may be included in the future.

Currently, there is a growing focus on cyber risks, which are considered among the most significant global risks for the financial sector and the economy as a whole. The information and communication technology (ICT) risks faced by enterprises are steadily increasing in both the frequency and severity of cyberattacks. Data breaches aimed at stealing personal information occur daily across the world, although only the largest incidents make media headlines.

Nevertheless, the use of artificial intelligence (AI) also offers a wide range of positive impacts:

Process automation and optimisation: AI enables the automation of routine tasks, accelerating workflows and increasing operational efficiency across various domains – from manufacturing to customer service.

Advancement of security technologies: AI enhances security systems by detecting anomalous behaviour and preventing cyberattacks and other data security threats.

EMERGING RISKS

Internal	External
› Disruption of procurement timelines › Risk of frequency spectrum loss › Regulatory risk › Decline in the Company's market share due to the sale of MTS	› Global geopolitical tensions › Scarcity of natural resources › Adverse impacts of artificial intelligence technologies › Technological threats and cybersecurity

DEVELOPMENT OF THE CRMS AND IC IN 2024

Continuous development and improvement of the CRMS and IC allows the Company to timely respond to changes in the external environment and internal business processes, improve the efficiency of its operations, and contribute to increasing shareholder value of the Company.

MAIN RESULTS OF CRMS AND IC DEVELOPMENT ACTIVITIES IN 2024

CRMS and IC development activities	Result
Development and improvement of the CRMS and IC methodology	› The Rules for the Identification, Assessment and Monitoring of Risks of Kazakhtelecom JSC were updated; › The Methodology for the Development, Implementation and Monitoring of the Key Risk Indicators System of Kazakhtelecom JSC was updated.
Development and implementation of an employee training programme	› To enhance employees' professional competencies, training seminars on risk management and internal controls were improved and conducted; › A video guide was developed on completing the Electronic Risk Database, including answers to frequently asked questions; › A training seminar on the corporate risk and internal control management system was held for risk coordinators of selected divisions of the Company.

MAIN RESULTS OF CRMS AND IC DEVELOPMENT ACTIVITIES IN 2024

CRMS and IC development activities	Result
Development of risk assessment apparatus using economic-mathematical models and expert opinions	› Quantitative risk assessment models were developed for selected risks; › The Methodology for Risk Assessment of Investment Projects was updated.
Improvement and maintenance of the Internal Control System	› The Guarantee Map of Kazakhtelecom JSC was updated; › Level 3 business process classifiers were developed in line with TMForum recommendations.

AREAS OF DEVELOPMENT OF THE CRMS AND IC

In the context of an unpredictable business environment where we face new challenges and high volatility, we recognise the need to continuously improve our risk management model and internal controls. We have clearly defined our objectives and direction based on fundamental concepts and standards. We are active to implement improvements and recognise where we are going and how to achieve our risk management and internal controls objectives.

Based on the following criteria:

- Corporate Governance and Culture;
- Strategy and goal setting;
- Operational Effectiveness;
- Monitoring and implementation of change;
- Information, communication and reporting;
- Control procedures.

INTERNAL AUDIT

The Internal Audit Service (hereinafter – IAS) is a body of the Company's Board of Directors that ensures the organisation and implementation of internal audit in the Company, directly subordinated and accountable to the Board of Directors and supervised by the Audit and Sustainable Development Committee.

The IAS operates in accordance with the Regulations on the Internal Audit Service and the Annual Audit Plans of Kazakhtelecom JSC.

In its activities, the Service is guided by the principles of independence, objectivity, competence, and professional attitude to work, as well as by quality standards and the standards of internal auditors' activities established by the International Standards for the Professional Practice of Internal Auditing of the Institute of Internal Auditors. In accordance with Standard 7.1 (Organisational Independence), the IAS complies with organisational independence.

As part of its core activities in 2024, in accordance with the Annual Audit Plan and the instructions of the Board of Directors, the Service carried out 15 audit events; the plan was fulfilled by 107%.

Based on the results of an independent external assessment of the IAS activities conducted by KPMG, it was confirmed that the IAS activities comply with the requirements of the International Standards for the Professional Practice of Internal Auditing in all material aspects. According to the assessment of compliance with the Standards' requirements, the IAS compliance rate made up 98%.