APPROVED BY

Minutes of the Board of Directors of PJSC ‘PIK Group’

No. 3 dated July 30, 2015

INTERNAL CONTROL AND RISK MANAGEMENT POLICY OF PJSC ‘PIK GROUP’

Policy

PT1001.0100.006.01-2015

APPROVAL SHEET

“Internal Control and Risk Management Policy of PJSC ‘PIK Group’” PT 1001.0100.006.01-2015

Initiator	Internal Audit Department

No.	Approving unit	Last name and initials	Signature	Date
1.	Director of the Internal Audit Department	E.A. Ivanova		

Distribution	□ limited □ confidentially □ for personnel □ open to the public

Developer in charge	Head of the risk division of the Internal Audit Department	A.V. Nasonova	

TABLE OF CONTENTS

TERMS AND ABBREVIATIONS

Terms and abbreviations used in this document shall be interpreted as follows:

PJSC ‘PIK Group’	Public Joint Stock Company ‘PIK Group’
PIK Group	PJSC ‘PIK Group’ and all its subsidiary and dependent companies (SDC)
Company	Public Joint Stock Company ‘PIK Group’ and all its subsidiary and dependent companies (SDC)
Internal control	a process carried out by the Board of Directors, Management, personnel and designed to provide reasonable assurance in achieving the Company’s objectives related to activities, reporting and compliance with laws and regulations
Risk management system	a process carried out by the Board of Directors, managers and other employees, which begins during the development of the strategy and affects all activities of an organization. It is focused on determining the events that can have an impact on an organization, managing the risks

	related to these events, as well as controlling that an organization's risk appetite is not exceeded and the reasonable guarantee of achieving an organization's objectives is provided.
Internal control subjects	the Board of Directors, Audit and Risk Committee, Management Board, Internal Audit and Risk Management Department, Business Units and employees of the Company, as well as all its subsidiary and dependent companies (SDC) responsible for performance of the internal control and risk management functions allocated to them (by internal documents of the Company).
Risk	probability of occurrence of an event which will have a negative impact on achievement of the Company's objectives
Risk probability	a possibility (determined by expertise) that a specific risk will ensue at a particular moment. It may vary from 0% to 100%.
Threat level	(amount of potential consequences of risk) an assessment of the financial loss connected with risk consequences, or estimate of costs for actions to liquidate consequences of the occurred risk in order to continue activities of the Company
Risk category	a group of risk causes. Risks are grouped in categories in the List of the Company's Basic Risks. Categories may contain sub-categories and smaller groups of risks
Risk cause (risk factor)	a condition that causes a specific risk. As a rule, risk mitigation (retirement) measures should be directed at the risk cause (factor)
Risk management strategy	short (several sentences) description of the main principles of the specific risk management. Main classes of strategy: risk aversion, risk acceptance, risk mitigation, risk transfer
Risk management measures	specific actions formulated by a person responsible for implementation of a specific risk management strategy. As a result of development of risk management measures, the period and expenses for implementation of a certain strategy are concretized.
Risk appetite	the risk level which the Company deems acceptable in creating the value of the Brand.

1. GENERAL PROVISIONS

1.1 The Internal Control and Risk Management Policy of PJSC 'PIK Group' is developed for the purpose of laying down uniform rules and policies for organization of the work in the field of building the Company's internal control and risk management system and developing the procedure for interaction of officers and business units of PIK Group for implementation of this procedure.

1.2 The Internal Control and Risk Management Policy is based on recommendations of the international standards, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO ERM 2004, COSO Internal Control), ISO 31000-2009 Risk Management. Principles and Guidelines.

2. PRIMARY OBJECTIVES AND TARGETS OF INTERNAL CONTROL AND THE RISK MANAGEMENT SYSTEM

The primary objectives of internal control and the risk management system shall be:

- strategic objectives which facilitate efficient management of operations and achievement of the Company's strategic objectives in the most effective way;
- operating objectives relating to efficient and effective use of resources and protection of assets;
- objectives in the field of assurance of reliability, correctness, integrity and actuality of financial, administrative and other information and reports of the Company;
- objectives in the field of compliance with the RF laws as well as requirements of the current regulatory documents and internal procedures of the Company;
- timely identification and analysis of risks in the Company's activities;
- analysis of conformity of the objectives of business processes, projects and business units with the Company's objectives;
- assurance of efficiency, reliability and integrity of business processes and information systems;
- control over creation of the required internal regulatory documents that regulate the Company's activities;
- assurance of reliability of procedures for counteracting illegal actions, abuse and corruption;
- identification of all risks that pose a threat to stability of operations, financial stability and achievement of the Company's strategic objectives;
- timely resolution of conflicts of interest arising in the course of the Company's activities;
- protection of assets;

- assurance of compliance with the requirements of laws and internal regulatory documents.

3. PRINCIPLES OF INTERNAL CONTROL AND RISK MANAGEMENT

- Internal control and the risk management system in the Company are based on the following principles:
- 'Tone at the Top' principle. The Board of Directors and the Company's management shall show the importance of ethical values at all levels of the organization (by means of instructions, actions, behavior) for the purpose of ensuring effective operation of internal control and risk management;
- Continuity principle. Internal control and risk management represent a continuous process covering the entire organization;
- Responsibility principle. All internal control and risk management subjects shall be liable for identification, assessment, analysis and monitoring of risks, as well as proper performance of control functions within their competence;
- Integrity principle. It represents the coverage of all business processes of the Company at all management levels;
- Principle of unity of methodological procedures. Internal control and risk management processes shall be implemented based on common approaches and standards for all structural units of the Company;
- Principle of precise distribution of functional duties. Duties and responsibilities of the Departments and business units are distributed for the purpose of carrying out internal control and risk management;
- Principle of risk orientation. Risk management shall deal with risks in each business unit so that the Company's top management could consider the entire risk portfolio and determine whether the residual risk portfolio of the Company meets its risk appetite in achieving the objectives;
- Principle of equation. Control functions shall be provided with tools and powers for their performance;
- Principle of priority. Control procedures shall be established in the fields of an organization's activities in the order of their criticality for successful operation of the Company;
- Principle of constant development and improvement. The risk management system shall be improved on an ongoing basis for identification of all possible risks of the Company's activities and the most effective application of risk management methods.

4. LIMITATION OF INTERNAL CONTROL AND THE RISK MANAGEMENT SYSTEM

- The achievement of the Company's objectives is influenced by limitations incidental to all management processes1:
- Subjectivity of judgment — the efficiency of the Company's internal control and risk management is limited by subjective decision-making;
- The risk management system may fail — wrong interpretation of instructions by personnel, wrong decisions based on wrong judgment, errors due to negligence, distraction or fatigue;
- Conspiracy of two and more persons who act together to commit an offense or conceal their actions;
- Expenses and benefits — the excessive control as well as allocation of valuable limited resources for control over insignificant risks are too costly and non-productive solutions for the Company.

5. ROLES AND RESPONSIBILITIES OF INTERNAL CONTROL AND RISK MANAGEMENT PARTICIPANTS

General participant interaction chart

Board of Directors and Audit and Risk Committee
Assessment of the efficiency of the risk management system Key Risk Report
Review of environment Approval of strategy
Determination of strategic actions
Vice-Presidents and Directors of Departments
Assessment of adequacy of mitigating measures
Monitoring of indicators of key risks
Business Units
Emerging Risk Report

[1] COSO Enterprise Risk Management – Integrated Framework. 2004

Identification, assessment, monitoring of operating risks
Performance of strategic actions
Key Risk Report

- The Company's Board of Directors shall approve the Internal Control and Risk Management Policy and assess its efficiency. It shall be responsible for approval and periodic review of the internal control and risk management strategy.
- The Company's Audit and Risk Committee shall give a general assessment of the efficiency of the internal control procedures in the Company (including based on reports of the Internal Audit and Risk Management Department).
- Division Vice Presidents of the Company shall be responsible for implementation of this Policy approved by the Board of Directors, as well as for operation and efficiency of the internal control and risk management procedures in the Company. The responsibility for operation and efficiency of the internal control and risk management procedures at lower management levels shall be borne by heads of Business Units.
- The Internal Audit Department shall develop risk management policies, methods and procedures in accordance with the best practice criteria and approaches. It shall collect, process and analyze the risk identification information received from the Company's Business Units and hold interviews with Division Vice Presidents. It shall generate and edit the Company's risk register, develop the risk management reporting system and revise it as and when necessary.
- Directors/Heads of the Company's Business Units shall implement this Policy and control the compliance with its provisions in the accountable business unit. They shall identify risks in the accountable business unit and participate in the expert assessment of risks.

6. COMPONENTS OF INTERNAL CONTROL AND RISK MANAGEMENT PROCESSES

The internal control and risk management processes in the Company shall consist of eight interconnected components. Their scope is determined by the managerial method used by the management; therefore, these components shall form a constituent part of the managerial process. These components shall include:

- internal environment;
- identification of objectives;
- determination of events;
- risk assessment;
- risk response;

- control means;
- information and communication;
- monitoring.

6.1 Internal environment

The internal environment has an impact on determining the strategy and identifying objectives of the Company, organizing business processes, as well as on the way risks are identified, assessed and managed. The internal environment has an impact on organization and operation of control means, information and communication systems, and monitoring.

The basic components that have an impact on the formation of the internal environment are:

- Management philosophy
    - the philosophy in the field of internal control and risk management is reflected virtually in all management activities of the Company's leaders. It is reflected in the corporate policy, verbal and written communication, and decision-making.
- Organizational structure
    - the organizational structure of the Company provides the basis for planning, performance, control and monitoring of its activities. The organizational structure of the Company includes
    - determining the key areas of powers and responsibility, as well as establishing subordination levels;
    - the organizational structure of the Company provides for efficient risk management, internal control and business operations that facilitate the achievement of the Company's objectives;
- Integrity and ethical values
    - the principles of integrity and ethical values are communicated to employees by means of the formalized Code of Conduct;
    - disciplinary measures are taken with respect to those employees who violate the code of conduct.
- Competence and standards in the field of personnel resources
    - the competence of the Company's employees reflects knowledge and skills necessary for the performance of tasks entrusted therewith;
    - standards apply to employment, positioning, training, assessment, assistance, promotion, remuneration and disciplinary measures, and specify the Company's expectations with respect to the level of integrity of employees, compliance by them with ethical rules and the level of their competence;
    - disciplinary measures indicate that violations of the rules of conduct are

unacceptable.

6.2 Identification of objectives

- management of the Company's risks is mainly focused on elaboration of consistent objectives and tasks within the entire Company, determination of key factors of success and risks, assessment of risks and determination of reasonable risk response methods, performance of actions aimed at removing risks, creation of the necessary control means;
- as part of managing risks, the Company's management not only chooses the objectives and sets them in such a way that they correlate with the Company's mission, but also makes sure they correspond to the risk level the Company considers acceptable, i.e. risk appetite.

6.3 Determination of events

It is identification of situations or events arising from operation of internal or external factors which have an impact on implementation of the strategy or achievement of the Company's objectives;

- the impact of events may be positive or negative. Events with a negative impact constitute risks. The Company's management assesses and develops measures for responding to events representing risks in order to
- prevent or minimize the impact of these events to an acceptable level. Events with a positive impact constitute opportunities; they are taken into account by the management in forming the strategy and identifying objectives.

6.4 Risk assessment

- risk assessment represents a process of analysis of risks and their consequences for the purpose of subsequent risk management, including risk removal and introduction of the required control procedures.

6.5 Risk response

- based on the results of assessment of the relevant risks, the Company's management determines the risk management strategy. In making a decision on risk response, the management considers the impact of this response on the probability and degree of risks, the correlation between expenses and advantages, and selects the response option which ensures that the residual risk stays within the limits of the acceptable level of risk appetite.

6.6 Control means

The following control means shall be used in the Company:

- security management. Procedures for control of access, including network access restriction, to databases and to certain levels of applications by means of passwords;
- procedures for control of user accounts and
- the respective rights help to set user access only to those applications or functions which

are necessary for the performance of strictly determined roles of these users;

- review and analysis of operating data. A number of control procedures to check the accuracy, completeness and correctness of information is carried out. The actual data is compared with the budget, forecast and previous data. The control means also include correlation of various types of data (operational or financial), conduct of investigations and removal of deficiencies;
- protection of assets. Equipment, inventories, monetary funds and other assets are physically protected and regularly recalculated and compared with the amounts recorded in check registers;
- distribution of powers. Duties are distributed among various persons in order to mitigate the risk of error or fraud. The duplication of functions is not allowed in the Company;
- control over operation of information systems. Control procedures are applied during determination, acquisition, installation, configuration, integration and maintenance of systems. Control procedures include service agreements which ensure proper operation of systems, as well as business continuity planning which, in its turn, ensures uninterrupted operation of information systems, tracking of the network infrastructure performance. System software control procedures also include tracking of incidents fixed by the system, logging, review of reports with the description of the use of data modification applications.

6.7 Information and communication

- the necessary information in the Company is determined, fixed and transferred in such form and within such time frames which make it possible for employees to perform their functional duties;
- information systems use both the internal data and the data from external sources, providing employees with sufficient information for managing risks and making decisions on achieving the objectives;
- to maintain efficient risk management, the Company fixes and uses the data from previous and current periods;
- the information infrastructure provides for collection and reflection of the data within such time frames and with such level of detail as is required by the Company for risk identification and assessment as well as risk response in such a way as to stay within the limits of the acceptable risk;
- to ensure the quality of information, the Company developed data control programs that apply to the processes of acquisition, maintenance and distribution of the relevant information and cover all levels of the organization;
- internal communication. The management distributes specific and targeted information on

its expectations concerning the risk management philosophy in the Company;

- external communication. The Company adjusted an effective exchange of information with external parties: clients, suppliers,
- regulatory bodies and shareholders;
- communication means. Information is distributed within the Company in such forms as release of regulations, policies, electronic messages, local intranet.

6.8 Monitoring

- monitoring of internal control and the risk management system is aimed at controlling the dynamics of changes in characteristics of risks and efficiency of implementation of risk management measures. Monitoring is carried out in the course of day-to-day operations and by carrying out additional periodic checks approved by the Board of Directors' Audit and Risk Committee. Monitoring makes it possible to determine whether the risk management and internal control process gives reasonable assurance that the stated objectives may be achieved;
- the risk management is monitored by IAD employees by collecting the information on the dynamics of key risks and implementation of plans for introduction of risk management measures;
- the results of assessment of internal control and the risk management system are used in preparing a section in the Company's annual report, which reflects the issues of internal control and risk management.

7. REFERENCES

1) COSO-Internal Control Framework The Committee of Sponsoring Organizations of the Treadway Commission.

2) COSO- Enterprise Risk Management Integrated Framework The Committee of Sponsoring Organizations of the Treadway Commission.

3) ISO 31000-2009 Risk Management. Principles and Guidelines.

Record of Changes

No. of change	Change description	Date	Person Responsible	Signature
