POLICY

in the Area of Risk Management and Internal Control of KAMAZ Publicly Traded Company

1. General

1.1. The Policy in the Area of Risk Management and Internal Control of KAMAZ Publicly Traded Company (hereinafter referred to as the Policy) shall determine the aims, tasks and principles for the functioning of the risk management and internal control system of KAMAZ Publicly Traded Company (hereinafter referred to as the Company), the responsibilities and powers of the risk management and internal control system entities.

1.2. The Policy has been elaborated in compliance with the law of the Russian Federation, the Corporate Governance Code, the Charter of the Company.

1.3. The Policy has been elaborated for purposes of establishing one single approach to carrying out the internal control and risk management processes in the Company.

1.4. The Company shall regularly assess efficiency of the risk management and internal control system.

The Company shall strive to enhance efficiency and quality of internal control and risk management processes, to harmonize them in line with the needs of business and corporate governance.

1.5. The Policy shall be mandatory for application by all the structural divisions of the Company and is recommended for use by the organizations set up with the Company's participation.

2. Terms and Definitions

For purposes of the present Policy, the following key concepts shall be used:

2.1. Risk owner shall be Deputy General Director of the Company, head of a division reporting directly to the General Director of the Company whose strategic or operational targets are affected by this risk.

2.2. Key risk indicators shall be quantitative indicators of risk sources (factors).

2.3. Control procedures shall be measures, actions, procedures worked out to ensure that reasonable confidence is gained that response to the risk is made effectively, in due time and in coordinated manner at different management levels and allows probability of and/or influence of the risk to be reduced to acceptable level.

2.4. Control environment shall be the position, knowledge and actions by the entities of the risk management and internal control system of the Company with respect to the Company's risk management and internal control system as well as awareness of such system's importance for the Company's activities.

2.5. Risk shall be an effect of uncertainty on achievement of the aims set, by which shall be understood a deviation from the expected result or event (positive and/or negative).

2.6. Appetite for risk shall be residual potential damage or allowable level of the key risk indicator, which the Company is prepared to accept in a bid to accomplish its aim or mission.

3. Aims, Tasks and Principles of the Functioning of the Internal Control and Risk Management System

3.1. The aims of the internal control and risk management system shall be as follows:

3.1.1. Ensuring that the Company's strategy is implemented;

3.1.2. Conserving and efficiently using the Company's resources and potential, ensuring that the Company's operations are continuous and that its functioning is efficient;

3.1.3. Reducing the number of unforeseen events and losses in the Company's business operations;

3.1.4. Company's timely adaptation to changes in the internal and external environment;

3.1.5. Preventing abuse on the part of officials, precluding fraud.

3.2. The tasks of the internal control and risk management system shall be as follows:

3.2.1. Ensuring that reasonable confidence is gained as to achievement of the Company's strategic and operational targets;

3.2.2. Ensuring that the Company's financial and business operations are efficient and that the Company's resources are utilized economically;

3.2.3. Identifying the Company's risks and managing such risks;

3.2.4. Making sure that the Company's assets are safe and secure;

3.2.5. Making sure that the accounts (financial statements), statistical reporting, management reporting and other reporting of the Company are complete, full and true;

3.2.6. Control over compliance with the law as well as the internal policies, rules and procedures of the Company.

3.3. The principles of the functioning of the risk management and internal control system shall be as follows:

3.3.1. Continuity of the functioning and integration – the risk management and internal control system shall function on a continuous basis and shall be an integral part of the corporate governance system in the Company at all its levels, covering all the divisions and employees in their performance of their functions. The decision making processes shall be carried out subject to comprehensive assessment of risks inherent in decision implementation.

3.3.2. Holistic – the risk management and internal control system shall encompass all the activities of the Company's business and all the types of the risks arising within their framework. Control procedures shall exist in all the business processes of the Company at all the governance levels.

3.3.3. Complete responsibility – all the entities of the risk management and internal control system shall be responsible for detection, assessment, analysis and continuous monitoring of risks within the framework of their activities, for development and implementation of required action plans aimed at managing risks, for implementation of control tools, their use within the framework of their competence,

continual monitoring of efficiency of the action plans aimed at managing risks and control tools.

3.3.4. Distribution of powers and responsibilities – decisions relating to risk management shall be made at different governance levels of the Company depending on the risk importance. For each level there shall exist a threshold for decision making relating to approval of the list of risks, action plans aimed at mitigating risk and other decisions to be taken within the framework of risk management, which are the threshold value of potential consequences (damage) resulting from the risk onset, which, if exceeded, shall be escalated to a higher level. Responsibilities in respect of performance of the functions and in respect of control over their performance shall be delineated with a view to avoiding a conflict of interest in the employees' performance of their responsibilities.

3.3.5. Economic feasibility and efficiency – the Company shall analyze the ratio between costs incurred in implementing control procedures and/or in implementing action plans aimed at managing risks and the savings. The risk management and internal control system shall ensure economic effectiveness (cost-efficiency) of the control procedures and action plans aimed at managing risks.

3.3.6. Priority – reduction (mitigation) of unfavorable consequences and/or probability of risk onset (occurrence) shall be primarily made vis-à-vis the critical risks with the greatest probability that they may happen.

3.3.7. Cross-functional interaction and coordination – internal control shall be exercised on the basis of clear-cut and efficient interaction of all the entities of the internal control at all the Company's governance levels. The process of cross-functional risk management shall be based on collective (collegiate) decisions taken jointly.

3.3.8. Knowledge – the risk management and internal control system shall imply on-going interactive exchange of information within the organization: flow of information about decision making risks shall proceed from lower governance levels to higher ones, decisions to minimize risks as well as control over risk management shall spread from the higher governance levels to the lower ones.

3.3.9. Ongoing development and improvement – the risk management and internal control system shall be regularly improved upon in order to identify all the possible risks involved in the Company's activities and to maximally effectively apply the methods of control and risk management as well as adaptation to changes in the internal and external environment.

4. Structure of the Internal Control and Risk Management System

4.1. The structure of the risk management and internal control system shall be a multi-level structure and shall correspond to the organizational chart of the Company.

4.2. Referred to the entities of the risk management and internal control system shall be the following: the Company's Board of Directors, the Budget and Audit Committee of the Company's Board of Directors, the Company's Auditing Board, the Company's Management Board, the Company's General Director, the Company's

internal audit division, heads of the Company's structural divisions, the Company's employees.

4.3. Effective functioning of the risk management and internal control system shall be ensured through distribution of powers and authorities as well as responsibility of the risk management and internal control system entities:

4.3.1. The Company's Board of Directors:

– shall approve the Policy in the Area of Risk Management and Internal Control;

– shall review reports on organization and the functioning of the internal control system, risk management system and corporate governance system;

– shall pass decisions on other matters relating to the functioning of the risk management and internal control system.

4.3.2. The Budget and Audit Committee of the Company's Board of Directors:

– shall make a preliminary review of the Policy in the Area of Risk Management and Internal Control and shall submit proposals (recommendations) to the Company's Board of Directors regarding its approval;

– shall exercise control over reliability and effectiveness of the functioning of the risk management and internal control system, including assessment of efficiency of the risk management and internal control procedures and preparation of proposals on how to improve them;

– shall exercise control to make sure that accounts (financial statements) of the Company are full, accurate and true;

– shall make sure that the internal and external audit functions are performed on the basis of independence and objectivity;

– shall examine other issues bearing on the functioning of the risk management and internal control system.

4.3.3. The Company's Auditing Board:

– shall exercise control over the Company's financial and business activities;

– shall make independent assessment of the truthfulness of the data contained the Company's Annual Report, the Company's annual accounts (financial statements).

4.3.4. The Company's Management Board:

– shall approve the list of critical risks, action plans aimed at reducing these risks and the level of generally acceptable risk;

– shall consider reports on assessment of risks and action plans aimed at reducing them.

– shall carry out general coordination of risk management process.

4.3.5. The General Director of the Company:

– shall procure that an effective risk management and internal control system functions in the Company;

– shall procure that powers (authorities), responsibilities and liability are distributed among the executives of the Company's divisions for specific risk management and internal control procedures;

– shall procure that efficiency of the risk management and internal control system is monitored constantly.

4.3.6. The Company's structural division which carries out internal audit:

– shall make independent assessment of efficiency of the risk management and internal control system, the action plans aimed at managing risks;

– shall provide methodological support of the risk management process.

4.3.7. The Company's risk owners:

– shall ensure maintenance of the effective control environment within the framework of the business process and coordination of the activities pursued by performers of the control procedures in order to achieve the goals of the relevant business process;

– shall make sure that risks are identified and assessed in good time, a risk management method is selected, that action plans are developed in good time subject to the recommendations provided by the internal audit division, the external auditors of the Company, other interested parties and that fulfillment of action plans aimed at managing risks is organized, that risks are monitored on a regular basis;

– shall make sure that there is effective liaison in place with the internal audit division with respect to documents and reports established within the framework of the risk management activities and based on the results of the inspections conducted by the internal audit division.

4.3.8. The executives and employees of the structural divisions responsible for organization and the functioning of internal control:

– shall ensure development of effective internal control procedures, shall document, implement, monitor, assess sufficiency of the control procedures and develop internal control in the activities entrusted to them;

– shall ensure effective implementation of the control procedures and the action plans aimed at managing risks in accordance with their functional responsibilities and the requirements of the Company's local normative documents;

– shall make sure that their immediate superiors are appraised in due time of the new risks, of failure to fulfill or of it being impossible to fulfill control procedures, of the need to modify control procedures and the action plans aimed at managing risks.

5. Key Methods, Approaches and Procedures of Internal Control

5.1. The Company shall practice the following package of internal control methods and approaches:

5.1.1. Putting in place in the Company an effective control environment by means of measures and actions carried out by the management at all the governance levels aimed at preventing failure to fulfill internal control procedures;

5.1.2. Installing and fulfilling control procedures in all the Company's business processes;

5.1.3. The functioning of the system for monitoring efficiency of internal control procedures by means of periodic checks of how effective the control environment is and whether control procedures are performed;

5.1.4. Ensuring the functioning of the authorization system which allows clear delineation and demarcation of the limits within which the employees are to operate in the performance of their job responsibilities;

5.1.5. Ensuring that login accounts in respect of business operations are documented and systematized;

5.1.6. Restricting unauthorized access to the Company's property using physical methods of control and security of assets, documents, data in the information systems;

5.1.7. Conducting independent audits by the Company's Auditing Board, by the Company's internal audit division, as well as the divisions which perform control functions in the Company.

5.2. Key Internal Control Procedures:

5.2.1. Verifying data and comparative analysis of performance indicators, assessment of performance efficiency – checking accuracy, completeness, lack of contradiction and correctness of the information, obtained from different sources, analysis of whether actual financial and non-financial indices of the Company's performance correspond to the planned indices in order to estimate the degree to which the pre-determined targets have been met.

5.2.2. Authorization (agreeing, approving the document / transaction) – all the financial and business transactions (operations) within the Company must be approved or agreed (cleared) by officers within the remit of their competence in compliance with the existing local and normative acts of the Company. The entity which exercises control within the remit of its competence, shall check and validate truthfulness, completeness and lack of contradiction of the information contained in the document, its proper execution and its conformity to the local normative acts of the Company.

5.2.3. Control over the accounting and reporting system – checking for compliance with the accounting policy, maintenance of analytical accounts and turnover summaries, checking whether reflection of business transactions is full, timely and reliable.

5.2.4. Physical control tools / ensuring that the assets are safe and secure – procedures aimed at checking actual availability and physical count of assets and liabilities, reconciling with the accounting data and control over unauthorized access to property and assets (inventory inspection, ensuring security of assets, assigning employees who bear material liability).

5.2.5. Delineation (demarcation) of rights of access to information systems – use of software based physical control and tools of physical control over the information furnished by the Company's employees.

5.2.6. Automated procedures of entering and transforming the information – stencils and filters for input of data in electronic reporting formats, automatic computing procedures, built into data processing programs.

6. Key Methods, Approaches and Processes of Risk Management

6.1. The Company shall apply the following package of risk management methods and approaches:

6.1.1.Risk management shall be based on a system of clear, clear cut strategic and operational targets of the Company and shall be an integral part of all the organizational processes and decision making processes.

6.1.2. The Company's targets to be decided upon at the strategic level shall be decomposed or communicated to the level of targets with respect to business processes, project management activities and the activities pursued by the Company's structural divisions and the Company's employees.

6.1.3. The Company shall strive to create risk oriented corporate culture.

6.2. Key Risk Management Processes:

6.2.1. Determination of Targets:

Risk management shall be based on a system of clear, clear cut and measurable targets of the Company articulated by the shareholders and management of the Company.

Should risks be identified the Company's risk management system shall test the threat posed to achievement of the formalized targets and tasks of the Company.

6.2.2. Risk Identification:

Risk identification shall provide for events and factors (internal and/or external) to be ascertained which may have an effect on achievement of the company's targets. With regard to each risk (if possible), key risk indicators shall be established.

Risk identification shall be made at all the Company's governance levels. The risks identified shall be classified according to the type of activity, in which they occur and according to the sources of impact (internal or external).

The Company shall implement the procedures which are aimed at timely identification of and control over the events affecting achievement of the Company's targets, shall establish and track change in key risk indicators.

The Company shall consolidate the information about the risks, shall inform the interested parties about the action plans aimed at risk management.

6.2.3. Risk Assessment:

The risks shall be analyzed depending on the following two parameters – likelihood of their occurrence (onset) and the extent of consequences for the Company. Assessment of risk parameters may be of qualitative or quantitative nature.

Risk assessment shall be made with the projection horizon corresponding to the horizon of meeting the Company's relevant target: in implementing the strategic targets, 10 years shall be chosen as the time period for assessing likelihood of the risk arising, in implementing the business planning targets 1 year horizon shall be chosen.

Risk likelihood shall be an expert based metrics and shall be determined as follows:

Table 1. Scale for Determination of the Risk Likelihood

Likelihood	Assessment of Likelihood	Description of Likelihood That Risk May Set In
low	less than 10%	likelihood of the event happening during the planned period is small.
medium	from 10 to 50%	the event is likely to happen but it is expected to be more likely not to happen during the planned period.

higher	over 50%	it is expected that the event is more likely to happen during the planned period.

Materiality of Risk shall have two scales: financial and reputational.

Table 2 Scale for Assessment of Risk Materiality

Materiality of Risk (consequences)	Amount of Damage Per Year *	Risk Management Level
critical	over 5 % of revenues	Company's Management Board
essential	from 0.5% - 5% of revenues	Company's General Director
significant	from 0.05% - 5% of revenues	Risk owner
misc	less than 0.05% of revenues	

* in respect of one risk

Table 3. Scale for Assessment of Impact on the Company's Reputation

Impact on the Company's Reputation	Potential Consequences (Damage)
occurrence of the risk would considerably affect the reputation which would reduce the share price by 5% to 15%	Essential
occurrence of the risk would considerably affect the reputation which would reduce the share price by more than 15%	Critical

Risk shall be assessed in such a way as to eliminate possible duplication of risk consequences caused by cross effects resulting from cross functional and other risks. The results of risk assessment shall be regularly revised.

6.2.4. Response to risks:

The Company shall use different methods of risk assessment depending on risk specifics and applicability of these or those assessment methods:

Key Methods of Risk Management:

– risk acceptance (the Company undertakes to eliminate possible consequences of risk situation onset and is prepared to cover the losses at its expense);

– avoiding (dodging) the risk (abstaining from the activities connected with the risk, i.e. refusal to perform any operations/to make any investments);

– transferring (distributing) the risk (decision to transfer the risk depends on the nature of activities, importance of the operation connected with risk and its financial significance. Standard mechanisms of risk pass-through shall include: insurance, transfer of risks to partners, outsourcing, diversification of operations, hedging);

– control of / reduction (minimization) of the risk (control over the level of risk (regular analysis of information about risks), taking measures to reduce probability of the risk event happening and/or to reduce possible damage).

Based on the results of assessing the risks identified, the Risk owner shall opt for a management strategy for this or that risk, shall devise and implement action plans aimed at managing risks. When choosing the risk management strategy and specific action plans aimed at managing risks, the Company shall be guided by the principle of economic feasibility and efficiency and observance of the level of appetite for risk approved by the Company.

6.2.5. Information and Communication

The information about risks shall be used in the decision making process. Reporting of the risk management system shall ensure that the risk management tasks are dealt with and shall be designed for fully-fledged and transparent exchange of information about risks.

6.2.6. Monitoring risk management:

Monitoring of risk management shall be done using control over risk trend development and efficiency of implementing action plans aimed at managing risks, by tracking the values of the key risk indicators. The Company shall regularly update the information about risks, risk management action plans, action plan completion status.

7. Operation of the Policy. Procedure of Introducing Amendments and Addenda to the Policy

7.1. The Chief of the Company's structural division which performs internal audit shall periodically consider the issue of whether it is necessary that amendments be made to the present Policy.

7.2. Amendments and addenda to the present Policy can be made by the decision of the Company's Board of Directors.

The Company's Board of Directors can terminate the operation of the present Policy and adopt a new Policy in the area of risk management and internal control.

7.3. In the case of contradiction between the norms of the law of the Russian Federation and the present Policy, the norms of the existing law of the Russian Federation shall apply.