# **PURPOSE AND GENERAL PROVISIONS**

## The Internal Control System Regulations of JSC NC “KazMunayGas” (hereinafter the Regulations) are developed to implement the Internal Control System Policy of JSC NC “KazMunayGas” (hereinafter the Policy).

## The Regulations define the interfaces, roles and responsibilities for the management, operation, performance and development of the internal control system (hereinafter the ICS) of JSC NC “KazMunayGas” (hereinafter KMG).

## The ICS is focused on business process review, timely identification and analysis of process-level risks inherent in KMG’s activities, and definition and analysis of control procedures to manage these risks.

## The ICS is integrated into the core and supporting business processes of KMG and includes procedures for immediate reporting to the Management of the appropriate level on any significant control gaps and weaknesses, along with the details of corrective actions that have been or should be taken.

## The ICS is an integral part of KMG’s corporate risk management system process.

# **SCOPE**

## These Regulations shall be applied by the entities of KMG’s ICS when carrying out activities in three key areas of the ICS:

###### performance improvement;

###### preparation of complete and reliable financial statements;

###### compliance with the RoK laws and KMG’s internal documents.

## Interfaces, roles and responsibilities for the management, operation and performance of KMG’s ICS are defined by the relevant regulations developed and approved by KMG’s SDEs in accordance with these Regulations.

# **DEFINITIONS AND ABBREVIATIONS**

## These Regulations use the following terms, definitions and abbreviations:

|  |
| --- |
| **business process** is a complex of interrelated actions initiated by a certain situation and resulting in a pre-known outcome that is significant for KMG, shareholders or individual SDEs; |
| **flowchart** is a graphical description of purposeful interrelated actions (steps) of a business process and their interaction with Business Process Owners. The flowchart shows individual actions (steps) in the form of blocks of various shapes connected by lines indicating the sequence and including the input and output steps; |
| **risk likelihood** is a measure (degree) of the possibility of a risk in a certain period of time;  **Business Process Owner** is KMG’s business unit in charge of the management, implementation, outcomes and effectiveness of a certain process, and management of documents describing this process in accordance with the approved process catalogue;  **risk effect** is the level of potential damage (loss) or impact of the risk/risk factor; |
| **SDEs** is subsidiaries and dependent entities, including jointly controlled entities and joint ventures of KMG; |
| **control design** is the description of how to perform the control, which should include the following mandatory elements: controller;control actions;control frequency and duration;control facilities (equipment, IT systems, documents and reports);control outcome. |
| **controller** is a business unit or an employee in charge who performs controls and actions aimed at reducing the risk likelihood and/or mitigating the risk within the business process;  **Assurance Map** is a document that defines the roles and responsibilities of ICS entities and other stakeholders for the performance assurance of KMG’s business processes, risk management and internal control between the three lines of defence; |
| **Business Process Classifier** (for the purpose of these Regulations) is a document that describes the structure of business processes implemented at KMG in three key areas (operations, preparation of financial statements and compliance with statutory and regulatory requirements) and enables ranking of business processes by the materiality of each business process; |
| **Audit Committee** is an advisory body of KMG’s Board of Directors, established to review the most important issues and advise KMG Board of Directors and KMG executive body within its competence defined by the Regulations on the Audit Committee of KMG’s Board of Directors;  **Risk Committee** is an advisory body under KMG’s Management Board, established for preliminary review of risk management issues of KMG and its SDEs and advising of KMG’s Management Board on them for making the necessary decisions;  **Company** is the collective name of Joint-Stock Company “National Company “KazMunayGas” and its SDEs;  **corporate-level control (CLC)** is control exercised by KMG’s bodies and Corporate Centre to minimise a corporate-level risk in order to reach reasonable assurance of KMG’s achievement of its goals (strategic, operational, reporting goals, legal compliance, etc.);  **control** (for the purpose of these Regulations) is an action defined by policies and procedures performed by a business unit and/or employees of KMG, or a system configuration aimed at reducing the likelihood of possible risks, preventing errors or mitigating risk events within the business process; |
| **risk and control matrix** is an internal document containing a list of risks and controls covering these risks, as well as their accompanying attributes;  **corporate-level risk and control matrix (CLRCM)** is a document defining corporate-level controls with a description of their key features;  **Three Lines of Defence Model** is a model that coordinates the processes of risk management and internal control by clearly defining and differentiating the roles and responsibilities between three separate groups: business functions, risk monitoring and internal control function, independent risk management and internal control performance evaluation function; |
| **Business Unit in Charge** is KMG’s business unit in charge of the operation of the ICS and corporate risk management system, improvement of ICS methodology and monitoring of best practices, as well as initiation of the compilation and update of the corporate-level risk and control matrix;  **Management Board** is a collegial executive body of KMG that manages its day-to-day operations; |
| **core processes (business processes)** are processes that create value for KMG, such as: Upstream, Oilfield Service, Oil Transportation, Oil Refining and Marketing, Gas Transportation, Gas Refining and Marketing;  **supporting processes (business processes)** are processes that support the core processes and management processes that do not create value for KMG but are necessary for effective management, such as: Legal Support; Procurement of Goods, Works and Services (Purchase); IT Support; HSE; Administrative Support, etc.;  **reasonable assurance** is a reasonable guarantee of achieving KMG’s goals, but not an absolute guarantee due to the inherent restrictions of the external and internal environment;  **risk** is the possibility of an adverse event that will negatively affect the ability to successfully achieve strategic goals;  **Risk Coordinator** is an employee of a business unit appointed to be in charge by the Risk / Risk Factor / Business Process Owner, whose duties include managing and coordinating risk / risk factor management efforts and internal control in his/her business unit and interacting with the Business Unit in Charge;  **corporate-level risk** is a risk that has an impact on the entire business of KMG, and is managed by KMG’s bodies and Corporate Centre with CLC;  **Risk Register** is a unified form of records for the KMG Group, which is used to identify, assess, re-evaluate, monitor production/non-production risks at all levels of risk management; |
| **Internal Control System (ICS)** is a set of processes and procedures, behaviours and actions that contribute to effective and efficient activities aimed at reasonable assurance of achieving KMG’s goals in three areas and minimising process risks in the implementation of activities;  **Internal Audit Service (IAS)** is KMG’s body that monitors economic and financial activities of KMG, conducts internal control and risk management evaluations, monitors compliance with corporate management documents and advises to improve the performance of KMG; |
| **Board of Directors (BoD)** is KMG’s management body that has overall charge of KMG’s activities, other than that within the exclusive competence of the General Meeting of Shareholders and the Management Board of KMG as prescribed by the RoK laws and/or KMG’s Charter;  **ICS entities** are bodies, business units and employees of KMG in charge of the management, operation and performance evaluation of the ICS;  **Fund** is Sovereign Wealth Fund Samruk-Kazyna JSC. |

# **RESPONSIBILITY**

## The Board of Directors shall be responsible for:

###### creating and operating an effective ICS at KMG;

###### identifying areas of improvement for the ICS;

###### monitoring the compliance with the ICS Policy;

###### analysing ICS performance;

###### reviewing IAS and external audit reports on IAS performance;

###### maintaining the independence of all ICS entities and the three lines of defence model;

###### demonstrating high standards of ethics and conduct to all employees of KMG;

###### setting the tone from the top by creating a risk culture and an environment that encourages and promotes reliable communication and effective cooperation between the three lines of defence;

###### setting KMG’s short- and long-term goals and objectives in the field of internal control and risk-based approach to ICS performance evaluation;

###### approving KMG’s internal documents defining the organisation, strategy of development and improvement of KMG’s internal control system;

###### ensuring support and involvement from ICS entities, identifying the main steps and those in charge of each step, continuous communications between ICS entities.

## The Audit Committee shall be responsible for:

###### preliminary review (before approval by the Board of Directors) of KMG’s internal documents defining the organisation, strategy for the development and improvement of KMG’s internal control system, Internal Control Policy and subsequent amendments thereto;

###### preliminary review (before review by the Board of Directors) of the results of the internal control system performance (maturity) evaluation according to the IAS report on the internal control system performance (maturity), and third-party independent assessment reports;

###### ensuring the reliability, effectiveness and further improvement of the ICS;

###### reviewing and analysing internal and external auditor’s reports on the ICS status.

## The IAS shall be responsible for (in accordance with the Internal Audit Service Regulations, including, but not limited to the following):

###### evaluating the adequacy and performance of the ICS;

###### timely testing the efficiency of controls;

###### timely reporting to the Board of Directors on the current state of the ICS at KMG.

## The Management Board shall be responsible for:

###### implementing the ICS Policy approved by the Board of Directors;

###### taking measures to improve internal control processes and controls, reliable and effective operation of the ICS;

###### monitoring the ICS;

###### improving the internal control processes and procedures;

###### defining the structure, line of subordination, corresponding authorities, roles and responsibilities.

## Business Process Owners shall be responsible for:

###### timely development, documentation, implementation, monitoring and improvement of controls in KMG’s business areas assigned to them;

###### timely development/update of process flowcharts, risk and control matrices;

###### preparing an action plan for further improvement of the ICS;

###### timely communication of information on the ICS to the employees of their business unit;

###### performance of controls (i.e., controls should give confidence in achieving the actual result, reliability of reporting, efficiency, compliance);

###### timely and complete implementation of corrective actions.

## The Business Unit in Charge shall be responsible for:

###### timely development/update and duly approval of ICS internal documents;

###### control design performance review;

###### timely approval of risk and control matrices and business process flowcharts;

###### compiling and updating the CLRCM;

###### monitoring the implementation of corporate-level controls;

###### providing methodological support to Business Process Owners in identifying and assessing process risks, as well as in developing, documenting, implementing, monitoring and improving controls;

###### preparing a Control Design Performance Review Report with recommendations (suggestions) for the elimination of identified violations, gaps, duplications of controls, etc. using the KMG-F-2726.2-37/RG-3209.2-37 form;

###### coordinating the implementation, methodological support and operation of the ICS in SDEs;

###### performing the ICS implementation, review and monitoring function within its competence.

## The Risk Committee shall be responsible for:

###### preliminary approval of the ICS schedule;

###### preliminary approval of flowcharts and risk and control matrices.

## The Risk Coordinator shall be responsible for:

###### interacting with the Business Unit in Charge when approving flowcharts and risk and control matrices;

###### identifying, assessing/reassessing risks / risk factors of his/her business unit;

###### providing methodological support to Business Processes Owners and interacting with the Business Unit in Charge in terms of approving documents.

## KMG’s employees shall be responsible for:

###### managing and taking ICS actions in accordance with the official duties assigned to them by job descriptions and/or internal documents;

###### timely identification and analysis of KMG’s business risks;

###### updating the description of business processes, including controls;

###### monitoring the operation of the ICS in their areas of activity, and independent self-evaluating of the performance of the internal control process that they manage and/or implement;

###### reporting to the Management on any committed or possible errors/gaps that have led or may lead to potential adverse events in business processes;

###### improving their skills in the field of ICS, including training in accordance with approved programs.

# **PROCESS DESCRIPTION**

## Planning

### Step 1. Business Process Classifier Development and Update

#### The business process classifier (hereinafter the Classifier) shall be developed and updated by the Business Unit in Charge at least once every three years or in case of a significant change in business processes by 15 October of the year preceding the planned one. The Classifier shall be developed/updated using the KMG-F-3210.2-37/RG-3209.2-37 form hereto based on:

###### KMG’s Business Process Catalogue (if any);

###### review of the approved Corporate Risk Register of JSC NC “KazMunayGas” using the KMG-F-2049.1-37/PR-251.3-37 form and Risk Map using the KMG-F-988.3-37/MD-986/3-37 form;

###### interviews with Business Process Owners (if necessary);

###### review of IAS reports based on previous audits.

#### The Classifier contains the following information: name of the business unit, name of the business process, category of the business process and business process rating (score based on the risk register, impact on the financial statements, impact on operations, impact on legal compliance, the final average weighted score).

#### When the Classifier is compiled, business processes shall be divided into two categories: core processes and supporting processes.

#### Based on KMG’s current business process catalogue (if any), the Business Unit in Charge, jointly with the Business Process Owner, shall rate each business process by its criticality. The rating shall be made in four categories. The rating categories and criteria are listed in Table 1.

**Table 1. Business Process Rating Criteria in the Business Process Classifier:**

| Rating Categories | Criteria |
| --- | --- |
| Rating on the basis of the Risk Register shall be based on the criticality score from KMG’s Risk Register | 1 — from 0 to 1;2 — from 1.01 to 8;3 — from 8.01 to 15;4 — from 15.01 to 28;5 — from 28.1 to 40. |
| Impact on financial statements | 1 — no effect on financial statements / financial reporting in the event of interruption or improper execution of business processes;2 — effect on financial statements / financial reporting is minor;3 — effect on financial statements / financial reporting is moderate, there may be complaints from stakeholders;4 — major effect, penalties may be applied;5 — critical effect, lawsuits against KMG and investigations related to financial statements / financial reporting. |
| Impact on operations | 1 — no effect in the event of interruption or improper execution of business processes;2 — risk effects are minor, short-term interruption of operations, equipment repair;3 — risk effects are moderate and can be completely corrected, temporary shutdown of operations with minor losses;4 — in case of interruption or incorrect execution of business processes, temporary shutdown of operations with major losses;5 — in case of risk occurrence, the company will practically not be able to recover from the effects associated with this risk; long-term or complete shutdown of operations. |
| Legal impact | 1 — minor legal effects in the event of interruption or improper execution of business processes;2 — non-compliance with statutory requirements, improvement notices from government authorities;3 — investigation by government authorities, legal action by a third party;4 — prohibitive measures by government authorities (e.g. revocation of licenses), numerous lawsuits by third parties;5 — actions on the part of government or judicial authorities resulting in a complete ban on operations, liquidation of a legal entity and/or criminal prosecution of employees. |

#### If necessary, the Business Unit in Charge shall conduct an interview with the Business Process Owner and can adjust the rating.

#### Next, the final average weighted score shall be derived by calculating the arithmetic mean between the rating based on the Risk Register and the arithmetic mean between the three impact ratings.

#### After conducting interviews with Business Process Owners and calculating the final average weighted risk rating based on the scores produced for all business processes, the Business Unit in Charge shall rank them by criticality (from the most necessary from the point of view of ICS formalisation to the least necessary one) in accordance with the final average weighted risk rating.

#### Business processes that manage critical risks / risk factors (included in the red zone of the risk map) shall be identified as the most material (critical).

#### Based on the results of items 5.1.1–5.1.8 of these Regulations, the Business Unit in Charge shall send the developed Business Process Classifier to the Risk Committee for review and to the Management Board for approval by 30 November of the year preceding the planned one.

### Step 2. ICS Schedule Development

#### An ICS schedule (hereinafter the Schedule) shall be developed before 1 December of the year preceding the planned one based on the approved Business Process Classifier using the KMG-F-3211.2-37/RG-3209.2-37 form hereto.

#### The need for the development and/or update of risk and control matrices and business process flowcharts of KMG can also be determined based on the control design review by the Business Unit in Charge, performance testing of IAS controls, recommendations from internal and external auditors, third-party evaluations of independent consultants, KMG’s strategic goals, and instructions and priority ranking by the Management.

#### If necessary, Business Process Owners shall submit information/documents on the need for the development and/or update of risk and control matrices using the KMG-F-3215.2-37/RG-3209.2-37 form and KMG’s business process flowcharts using the KMG-F-3212.2-37/RG-3209.2-37 form to the Business Unit in Charge by 15 November of the year preceding the planned one.

#### When preparing the Schedule, the deadlines for the development and/or update of risk and control matrices and flowcharts shall be set no later than 15 November of the year preceding the planned one.

#### The Schedule shall be sent to the Risk Committee for review and approved by the Management Board by 31 December of the year preceding the planned one.

#### The Business Unit in Charge shall send the Schedule to the relevant Business Process Owners for review within 3 (three) business days after the approval.

#### The Business Unit in Charge shall provide methodological support and coordinate the development and/or update of flowcharts and risk and control matrices by Business Process Owners and Risk Coordinators based on the approved Schedule, and review the control design performance.

## Formalisation of Business Processes

### Step 1. Flowchart Development and Update

#### Formalisation of business processes shall include a description of KMG’s existing business processes. The activity shall be formalised, including business process steps, the workflow between the action owners, as well as incoming and outgoing information, shall be described. This level of detail makes it possible to identify and analyse risks in processes and define controls. The formalisation of controls is one of the principles and conditions for the effective operation of the internal control system.

#### The flowchart shall be developed by the Risk Coordinator and agreed with the Business Process Owner in Microsoft Visio, ARIS or in similar business process modelling software.

#### The objects (graphic images) used in the flowchart shall match the objects in the KMG-F-3212.2-37/RG-3209.2-37 form hereto.

#### In accordance with the flowchart, the role, position and name of the business unit involved in the business process shall be indicated vertically in the left part of the flowchart.

#### The business process shall be detailed to process steps.

#### The sequence of controls when describing the process shall be indicated by connecting the main elements of the flowchart from the entry (beginning of the process) to the exit (end or output of the process). If there is a need to describe the controls of another process, it is advisable to give a reference to the flowchart of this process.

#### Objects indicating risks and controls shall have a name and unique numbering.

#### It is advisable to indicate the “Event” figure after each action (step) of the business process to leave the completion trace.

#### If there are logical operations (several options), depending on the type of logical operation, it is advisable to use the following figures in the flowchart: “and” — both options are true, “and/or” — only one or several options are true, “Exclusive” “or” — only one option is true.

#### If necessary, the flowchart can include a glossary with definitions.

#### The Risk Coordinator shall have the flowchart approved by the Business Process Owner and send the approved business process flowchart to the Business Unit in Charge to be reviewed for compliance with the flowchart requirements.

### Step 2. Risk and Control Matrix Development and Update

#### The Risk Coordinator, jointly with the Business Process Owner, shall develop and/or update risk and control matrices based on the flowchart within the time specified in the approved Schedule, following items 5.2.12-5.2.28 hereof. The risk and control matrix is interconnected with the flowchart in terms of the general description of the business process and is an integral part of the flowchart.

#### The Business Unit in Charge shall provide methodological support and coordinate the development and/or update of risk and control matrices by Risk Coordinators and Business Process Owners.

#### The Risk Coordinator shall coordinate a draft risk and control matrix with the Business Process Owner and submit the draft to the Business Unit in Charge for approval.

#### The Business Unit in Charge shall review risk and control matrices submitted by Risk Coordinators and Business Process Owners for compliance with the requirements for them in accordance with the Schedule. During the review, the Business Unit in Charge can review the control design performance.

#### After reviewing the flowcharts and preparing risk and control matrices, the Business Unit in Charge shall send the risk and control matrices and process flowcharts in two languages to the Risk Committee for review and to the Management Board for approval by 31 December in accordance with the Schedule.

#### The Business Unit in Charge shall submit approved risk and control matrices and process flowcharts to the IAS.

#### The risk and control matrix shall be prepared by the Risk Coordinator jointly with the Business Process Owner in Microsoft Office Excel using the KMG-F-3213.2-37/RG-3209.2-37 form and shall consist of the following 3 areas: Name of the Business Process, Risk, Control.

#### The Name of the Business Process contains the following information: Process, Subprocess. Example of the core process: Process — Well Stock Management, Subprocess — Real-Time Production Accounting by Wells. Example of the supporting process: Process — Accounting of Funds, Subprocess — Entry of Bank Payments in the ERP System.

#### The Risk contains the following information about the risk: Process Step, Step Description, Risk Name, Code, Action Owner, Risk Description, Risk Likelihood, Risk Effect.

###### Process Step is an action/function within a subprocess where a process risk occurs. Example of the core process step: Recording of gas volume and losses in the accounting system. Example of the supporting process step: introduction of primary documents for the accounting of other reserves.

###### Step Description contains detailed information about the action/function within the subprocess where the process risk occurs.

###### Risk Name contains a brief description of the process risk.

###### Code is intended to assign an individual numeric serial number to each risk in the following format: R.XX.A, where R is the risk designation, XX is the abbreviation of the business unit, A is the risk number.

###### Action Owner contains information about the role, position and name of the business unit that owns the action.

###### Risk Description contains a detailed description of the risk, including risk factors that may negatively affect the achievement of the goals of the process under consideration, causes and effects of the risk.

###### Risk Likelihood shall be filled in by the Risk Coordinator and Business Process Owner, where the likelihood is assigned by an expert estimate for a certain period of time. Estimates shall be made for the following categories: low — the risk is unlikely, moderate — 50/50 probability, high — the risk is highly likely.

###### Risk Effect shall be filled in by the Risk Coordinator and Business Process Owner, where the potential damage is assigned by an expert estimate of the potential damage from the risk. Estimates shall be made for the following categories: low — minor losses within operating expenses, moderate — medium and major losses, high — serious, catastrophic losses.

#### Risk identification shall be based on the review of the detailed process description. The following information can be used for this purpose:

###### both approved and planned regulations, policies, procedures, rules, methods, standards, instructions for business processes of a business unit;

###### business process catalogue (if any);

###### RACI matrix;

###### findings and recommendations based on the internal audit of the IMS, IAS and external consultants;

###### business process and efficiency goals of business process employees of the business unit;

###### Risk Register;

###### other additional sources of information.

#### Risk identification shall take into account the circumstances shown in Table 2.

**Table 2. Circumstances Affecting the Occurrence or Change of Risks**

| **No.** | **Circumstances Affecting the Occurrence or Change of Risks** | |
| --- | --- | --- |
| 1 | Internal | * New personnel (new employees may have a different point of view on the internal control system or other priorities). * Introduction of new or changes in already used information systems (significant and rapid changes in information systems can also change the risks associated with the internal control system). * Rapid growth and development of a business entity (existing controls may not cope with the increased scope of operations and contribute to an increase in the risk of their inadequacy to new business conditions). * New business approaches, new types of goods, works, services (development of new types of operations, products, which the entity has little experience with, may give rise to new risks associated with the internal control system). * Reorganisation of the business entity may be accompanied by personnel downsizing and changes in roles and responsibilities, as well as in control functions performed by employees: they can also affect the risk associated with the internal control system. |
| 2 | External | * Changes in the business entity environment (macroeconomic changes, including those related to changes in the regulatory environment, may lead to changes in competitive pressure and to significant changes in risks). |
| 3 | External and Internal | * Expansion of operations abroad (expansion of business operations abroad and opening of subsidiaries, investments in foreign enterprises entail new and, as a rule, unique risks that may affect the internal control system, for example, additional or changed risks as a result of transactions with foreign currency, additional or changed risks due to the peculiarities of foreign, including tax, legislation). * New principles, standards, regulations, instructions in the field of accounting and reporting (the adoption of new accounting principles or their change may affect the risks associated with the preparation of financial statements). |

#### The Control is the description by the Business Process Owner of the existing controls covering the identified risks. To determine the existing controls, the Risk Coordinator and the Business Process Owner shall analyse a set of existing step-by-step actions aimed at minimising or managing risks and/or their effects and likelihood.

#### The Control contains the following information about the control: Name of Control, Code, Controller, Detailed Description of Control, Evidence of Control, Type of Control, Frequency of Control, Method of Control, Significance of Control, Financial Statement Assertions.

###### The Name of Control is an action/function within the subprocess where the control covering the identified risks is implemented.

###### The Code is intended for assigning an individual numerical sequence number to each control in the following format: C.XX.A.B, where C is the control designation, XX is the abbreviation of the business unit, A is the control number, B is the sequence number of control when it is duplicated. However, it should be borne in mind that several controls can be developed to minimise or prevent one risk.

###### The Controller contains the role, position and name of the business unit responsible for performing the specified control.

###### The Detailed Control Description contains detailed information about the control. In order to correctly and informatively describe the control, it is necessary to have answers to the following questions: what actions are taken during the control? how (by e-mail, by courier, in an IT system, etc.) is information transmitted during the control; from whom and to whom is information transmitted during the control; on the basis of which documents (internal regulatory or external) is the control performed; to whom are the control results reported; in which automated systems is the control recorded; what is required for the control? in case of approval and rejection, what happens next; if necessary, specify the transaction number, the report number in an IT system.

###### The Evidence of Control indicates information which makes it possible to determine the control execution and is necessary for reporting on the performance of the internal control system. Example of control traces: signatures, endorsements, seals, status, logs of operations in an IT system, orders, reconciliations, etc.

###### The Type of Control can be preventive or identifying. The preventive type of control means the implementation of preventive actions to prevent the risk. Types of preventive controls: limitation of authority (e.g. purchase amount limit); limitation of access (e.g. computer information system access control tools); archiving (e.g. maintaining an archive of business correspondence, primary documents, periodic archiving of databases); collective execution (e.g. decision-making by the budget committee); recording of operations (e.g. bookkeeping and management accounting); parallel execution of operations (e.g. transmitting information in electronic form with simultaneous transmission of the same information on paper). The identifying type of control helps to identify a particular risk after its implementation. Types of identifying controls: review of operations for compliance with internal documents (e.g. review by the Head of Business Unit for the correct filling in of documents); inventory (e.g. recalculation of funds, recalculation and evaluation of inventories, fixed assets, reconciliation with debtors and creditors); expert review — professional opinion of an independent expert (e.g. equipment condition assessment); performance review (e.g. the Head of Business Unit reviews the performance of an individual task by a newly recruited employee during and after the probationary period); information reconciliation (e.g. information from one report is reconciled with data from another).

###### The Frequency of Control determines the control interval: Annually, Quarterly, Monthly, Bimonthly, Weekly, Continuously. Where the Detailed Control Description column does not contain accurate data on the frequency of control, this field shall take the As Needed value. In this case, it is advisable to specify exactly when the Controller starts the control (e.g. after receiving a request from the manager and/or notification about the completion of a certain operation).

###### The Method of Control indicates how the control was performed. The method of control can be manual / semi-automatic / automatic. Manual controls are performed completely manually by the controller outside of information systems. Semi-automatic controls are performed automatically, but with the involvement of the controller. They shall be initiated or completed manually (e.g. signing a document on paper). Automatic controls are implemented in the information system without the involvement of employees. Control implies the implementation of control automatically in the information system according to a configured algorithm (e.g. the selection of values from a fixed list in the information system). Automatic controls are mainly preventive and prevent an incorrect/erroneous action.

###### According to the level of significance, controls may or may not be key. Key controls can be identified based on the following features: cover more control objectives than others; control exceptions and non-standard/non-routine operations; control areas at risk of fraud; control manual data entry into the system and data transfer between systems.

###### Financial Statement Assertions are intended to determine the adverse impact of risk on financial statement assertions of KMG. Financial statement assertions are explicit or implicit assertions made by the Company regarding the fundamental accuracy of the information contained in its financial statements, i.e. the Company claims that the data in its financial statements are a true representation of its assets and liabilities. Financial statement assertions are shown in Table 3.

**Table 3. Financial Statement Assertions**

| Financial Statement Assertions | Definition |
| --- | --- |
| Occurrence | Recorded business transactions, events and other facts of business life that actually occurred (transactions and events, submission and disclosure of financial statements). Example of a question: do the recorded assets actually exist? |
| Existence | Recorded transactions actually occurred on the reporting date (closing account balance). Example of a question: do the recorded operations really have results in the form of traces and documents? |
| Completeness | All transactions and events to be recorded are recorded (transactions and events, closing account balance, submission and disclosure of financial statements). Example of a question: is all the information really reported in the financial statement? |
| Cut-off | Transactions and events are recorded in the proper reporting period (transactions and events). Example of a question: are all the transactions valid in the corresponding reporting period? |
| Rights and obligations | Transactions and disclosures relate to KMG (submission and disclosure of financial statements). Example of a question: does KMG really have rights to the assets? |
| Evaluation and allocation | Assets, liabilities and equity included in the financial statements are measured appropriately, and cost allocation adjustments are reported correctly (closing account balance). Example of a question: are all balance accounts reported and evaluated correctly? |
| Accuracy | Transactions were reported in the corresponding amounts (transactions and events, submission and disclosure of financial statements). Example of a question: are all transactions reported correctly? |
| Classification | Financial information is presented properly (transactions and events, submission and disclosure of financial statements). Example of a question: are all transactions recorded correctly in the corresponding accounts? |
| Comprehensibility | All relevant information and disclosures are included in the company’s reports, and all information presented in the reports is reliable and easy to understand (submission and disclosure of financial statements). Example of a question: is the submission and disclosure described clearly for all its users? |

#### The following two methods of risk identification shall be used to identify process risks:

###### initial identification of risks, including performance analysis of similar companies, collection and analysis of statistical data, what-if analysis of the business process, individual expert estimates, group methods, and review of audit reports;

###### subsequent risk identification (risk identification during operations).

#### Risks with a simultaneously low likelihood and effect rating are not subject to further treatment and are not included in the risk and control matrix.

#### If necessary, the risk and control matrix can include a glossary with definitions.

#### For each control, it is necessary to perform a high-level analysis using the following questions:

###### is the control description sufficient?

###### whether the control is performed by the relevant person at the appropriate level. Does the controller have sufficient experience to perform effective control or does he/she have adequate authority?

###### is there a proper division of responsibilities?

###### is control performed at the appropriate step in the business process?

###### is control performed with a specified frequency? Is control too complicated to be performed with a specified frequency?

###### is there a proper trace (evidence) that the control is being performed effectively, enabling testing of the control?

###### are there clear criteria for determining whether the control has worked or not? If the control has failed, is there a proper procedure for establishing this fact and a procedure to correct the control failure?

###### is the risk of making an error when performing manual control acceptable and is it checked that it is properly covered by the appropriate identifying controls? If not, should the control be automated?

## Control Design Performance Review

#### Risk Coordinators and Business Process Owners, jointly with the Business Unit in Charge, shall review the control design performance in the context of the business process in order to:

###### get reasonable assurance that the operations are effective and serve to achieve KMG’s goals;

###### get reasonable assurance that KMG’s financial statements are reliable and fully reflect KMG’s financial standing;

###### get reasonable assurance that KMG complies with statutory and regulatory requirements.

#### If necessary, the control design performance review can be carried out separately from ICS formalisation within the time specified in the approved Schedule (after the flowchart and risk and control matrix are compiled).

#### Upon request, the Risk Coordinator shall submit all the necessary supporting information, documents, reports on the business process to the Business Unit in Charge within 5 business days for the control design performance review.

#### The control design performance review shall be based on the risk description and description of the current control covering this risk. The review shall cover the extent to which all identified risks are covered by the existing controls, whether the likelihood of possible risks is reduced, whether errors are prevented and/or errors are detected after they are committed, as well as whether there is redundancy or duplication. The absence or presence of controls that are not directly related to the identified risks means that this business process has a control point that is not covered by controls. In such cases, this may mean that this control is ineffective.

#### It shall also be determined to what extent the controls operating in the business process minimise the risks of this business process. The main purpose of this procedure is to determine whether the control, if it is consistently performed in accordance with the description and taking into account the actual implementation of the procedure in practice, is able to provide adequate coverage of the relevant risks.

#### The control design performance review shall be made using the KMG-F-2725.2-37/RG-3209.2-37 form hereto, which supplements the elements of the risk and control matrix with the following information: method of the control design performance review, quality of risk documentation, risk assessment accuracy, quality of control documentation, control design performance, control design review documentation, control object/respondent, controller.

###### Methods of the control design performance review include survey, monitoring, inspection, re-execution. Survey is interviewing the controller in order to find out how the control is performed, as well as what measures are taken by the controller in case of exceptions, control gaps, knowledge and expertise evaluation of the controller. Monitoring is monitoring of controller actions directly during the control being inspected. Inspection is the study of evidence of the proper implementation of the control being reviewed. For example, documentation review, review of verifications and identified nonconformities, and/or a full-scale inspection. Re-execution is the execution of control in accordance with its design and verification of the control outcomes. Since none of the methods gives absolute confidence in the correctness of the control, combinations of methods shall be used during testing.

###### The quality of risk documentation indicates whether all risks, their risk factors and effects have been determined, whether they have been sufficiently documented in accordance with internal documents. Correct shall be indicated if there are no comments. If there are comments, the justification shall be indicated.

###### Risk assessment accuracy indicates the correctness of determining the likelihood and effect of the risk. Correct shall be indicated if there are no comments. If there are comments, the justification shall be indicated.

###### The quality of control documentation indicates whether all controls have been determined, whether they have been sufficiently documented and in accordance with internal documents. Correct shall be indicated if there are no comments. If there are comments, the justification shall be indicated.

###### Control design performance indicates the control design performance rating: “I” (ineffective) — control objectives are not achieved, significant changes in the control design are required; “EM” (effective — medium level) — control objectives are achieved, but changes in the control design are required; “EH” (effective — high level) — control objectives are fully achieved.

###### Control design review documentation describes in detail the procedure itself, including a description of the achievement of the control objective, the reasons for the partial effectiveness of the control, the reasons for the ineffectiveness of the control.

###### Control object/respondent indicates the full name of the employee of the business unit undergoing the control design performance review.

###### Controller indicates the full name of the employee of the Business Unit in Charge who performed the control design performance review.

#### The control design performance review shall cover the following aspects:

###### relationship of controls and risks of business processes, i.e. whether business processes and their corresponding controls are effective in achieving the goals set by management and covering risks;

###### the ability of the control to prevent or detect events affecting the implementation of risks in a timely manner;

###### division of responsibilities for the business process under review;

###### timely resolution of issues and correction of nonconformities that are identified by the control;

###### whether there is duplication of controls and responsibilities of employees of the business unit;

###### reliability of the information used in the control.

#### If gaps are identified based on the control performance review, the gaps shall be discussed with the controller with recommendations for control improvement also agreed with the controller and Business Process Owner. The control is considered ineffective by design (reliability) if:

###### there is no control;

###### the control exists, but is not formalised;

###### the control does not completely cover the risk (the residual risk is higher than acceptable).

#### If the control design is rated as ineffective, or the corresponding control necessary to achieve the control objective has not been implemented, then the employee of the Business Unit in Charge jointly with the Business Process Owner and the controller shall:

###### identify compensating controls that can provide reasonable assurance that the relevant control objectives will be achieved, provided that such controls are effective;

###### if there are no appropriate compensating controls in the described risk and control matrix, recommendations shall be developed for the development and implementation of alternative controls.

#### If there is no control that minimises the risk, the Risk Coordinator, jointly with the Business Process Owner and the Business Unit in Charge, shall develop an effective control design and implement it as soon as possible. The control design shall be developed taking into account the following aspects:

###### the control design shall factor in the external and internal environment that affects KMG’s goals and operations;

###### controls shall be continuously improved and adapted to changes in the internal and external environment;

###### control shall be applied at KMG to reduce risks to an acceptable level;

###### the optimal combination of controls shall be determined by the Business Process Owner. For example, a significant risk may be covered by several controls, or a single control may cover several significant risks;

###### planning of controls shall be based on the ratio of costs for controls and possible damage caused by the risk. The costs of controls in combination with the costs of risk management measures shall not exceed the possible damage and effects caused by the risk.

#### In case of a request from KMG’s Management Board, the method of end-to-end testing of controls can be applied. End-to-end testing is a testing method performed by tracking a single procedure from beginning to end through verification and analysis of supporting documents specified in control procedures. This analysis shall be performed to ensure that the procedure and controls are properly documented and implemented. End-to-end testing shall be based on sampling. The sampling period is one year, the sample size depends on the control frequency and the rating of risks reduced by the control. If the control frequency is more than once a day, the number of samples will be 20, once a day — 15, weekly — 10, monthly — 3, quarterly — 2, annually — 1. If the control is automated, it is enough to test one operation. With a high-risk rating, the number of samples depending on the control frequency shall be multiplied by 2, with an average risk rating — by 1, with a low-risk rating — by 0.5.

#### The results of end-to-end testing shall be recorded and agreed with Business Process Owners. Control performance review testing can be documented both in electronic form and on paper, while the list of documents proving tests may include: record of the survey/interview, copies of documents, minutes and other documents, copies of print screens (screenshots). The Business Unit in Charge, jointly with Business Process Owners, shall develop an action plan to eliminate the identified gaps to be included in the Schedule and taken into account when updating risk and control matrices for the next year.

#### The control design performance review shall be documented in a report to be submitted to the relevant business units. The control design performance review report shall be issued using the KMG-F-2726.2-37/RG-3209.2-37 form. This report shall contain the following information: Summary for the Management and Business Process Owner, purpose and scope, results, constraints and conclusions.

#### This report includes the following for identified gaps in internal controls:

###### description of the internal control gap and the associated risk;

###### detailed description of actions to be taken to eliminate the gap;

###### action owner;

###### deadlines.

#### After a reasonable period of time after correcting the gap, the design effectiveness and performance (i.e., checking the actual performance) of controls that were previously recognised as ineffective shall be re-evaluated.

#### The control design performance review report shall also indicate the rating of the entire business process within the ICS indicated in Table 4.

**Table 4. Rating of Internal Control in Business Processes**

|  |  |  |
| --- | --- | --- |
| **Rating of Internal Control in Business Processes** | | **Description** |
|  | **5 — Adequate** | The main risks are managed at the proper level. All the tested controls are developed at the proper level and function effectively, minor gaps in the internal control system were identified. Business processes are managed efficiently and meet the expected goals. |
| **4 — Satisfactory** | The identified risks are not critical. Most of the tested controls are developed at the proper level and function effectively, some opportunities for their improvement were identified. Findings include some control system gaps. |
| **3 — Requires improvement** | High risks are not adequately controlled. Some controls are either not designed properly or do not function effectively. The control environment needs improvement in order to achieve the set objectives. Internal control system gaps require immediate attention from management. |
| **2 — Requires significant improvements** | Critical and high risks are not adequately controlled. Most controls are either not designed properly or do not function effectively. The control environment needs significant improvement in order to achieve the set objectives. Control system gaps require immediate attention from management. |
| **1 — Poor** | Critical and high risks remain absolutely unmanageable, there are serious control system gaps that can negatively affect the company’s operations and/or expose the company to significant financial and other losses. |

## Corporate-Level Risk and Control Matrix Development and Update

#### The corporate-level risk and control matrix is based on the five components of the ICS described in KMG’s ICS Policy:

###### control environment;

###### risk assessment;

###### controls;

###### information and communication;

###### monitoring procedures.

#### The Business Unit in Charge shall annually fill out CLRCM form KMG-F-3215.2-37/RG-3209.2-37 and duly submit it for approval to the concerned business units of KMG.

#### Business units shall duly submit their suggestions and additions to the draft CLRCM to the Business Unit in Charge within 10 business days.

#### The Business Unit in Charge shall make adjustments to the draft CLRCM based on the review.

#### The Business Unit in Charge shall submit the draft CLRCM reviewed by all business units/IAS to KMG’s Management Board for approval annually before the 30th day of the month following the reporting year, thereby submitting reports on the status of KMG’s corporate-level controls.

#### The remaining columns of the CLRCM specified in Table 5 shall be out in accordance with these components.

**Table 5. Columns of the Corporate-Level Risk and Control Matrix**

| **No.** | **Column** | **Description** |
| --- | --- | --- |
| **1** | ICS components | ICS components according to KMG’s ICS Policy. |
| **2** | Principles | 17 COSO principles. |
| **3** | Risk code | A unique corporate-level risk number. |
| **4** | CL risk name | Brief description of the corporate-level risk. |
| **5** | CL risk description | Detailed description of the corporate-level risk, including risk factors that may negatively affect the achievement of the goals of ICS component under consideration, causes and effects of the risk. |
| **6** | CL control code | Corporate-level control number. |
| **7** | CL control owner (role) | Employee / Business Unit / Committee in charge of CLC. |
| **8** | Detailed description of CL control | Detailed description of CLC, including actions, systems, documents, criteria necessary for implementation/compilation to reduce corporate-level risks for the corresponding ICS Component. |
| **9** | Type of CL control | * preventive — if the control works before the risk occurs and prevents it; * identifying — if the control works after the risk has occurred and can identify the risk effects. |
| **10** | Frequency of CL control | This column indicates the frequency of control: Annually, Quarterly, Monthly, Bimonthly, Weekly, Continuously. |
| **11** | Method of control | This column indicates the method of control — manual, semi-automatic, automatic. |
| **12** | Document regulating this CLC (item) | A document (possibly with an indication of the item) that describes the responsibility/obligation to perform control. |
| **13** | Current status | * in process; * to be implemented; * to be changed. |

## Control Efficiency Testing

#### The IAS shall develop control efficiency testing plans for significant business processes in accordance with the approved IAS work plan for the corresponding year and based on KMG’s approved risk and control matrices.

#### In accordance with the approved IAS work plan for the corresponding year, the IAS shall test the performance of controls for significant business processes, based on the results of which it shall provide an independent performance evaluation of controls. If necessary, IAS shall request additional information from the relevant Business Process Owners to confirm the conclusions in the risk and control matrices.

#### After control efficiency testing, the IAS shall prepare an Audit Report and submit it to KMG’s Board of Directors for review.

#### The Business Unit in Charge may be involved in control efficiency testing as instructed by KMG’s Management Board.

## Information and Communication

#### Information and communication is a process of identifying, documenting and timely communicating the necessary and relevant information to Business Process Owners and Management.

#### Information support and communication systems include the following:

###### information collection, processing and communication system, including reports and messages containing information on all significant aspects of KMG’s operations;

###### effective communication channels and facilities that provide vertical and horizontal communication links within KMG and with subsidiaries and dependent entities and third parties;

###### due access and safety of information obtained from internal and external sources;

###### communicating the current documents used at KMG to employees.

#### The information support system within the ICS is represented by the following tools:

###### ICS Policy and Regulations;

###### Business Process Flowcharts;

###### Business Process Risk and Control Matrices;

###### Control Design Review Reports;

###### ICS Performance (Maturity) Evaluation Reports;

###### ICS Improvement Plans (if necessary).

#### The Business Unit in Charge shall provide access to ICS documents for the employees of KMG and its SDEs.

## Monitoring

#### Internal control monitoring is considered a necessary tool for maintaining the ICS at the required level of performance and reliability. Monitoring is a process of evaluating the components of the ICS, which makes it possible to assure that KMG is achieving its goals.

#### The main requirements of KMG in the field of internal control monitoring include:

###### continuous and periodic performance evaluations of the ICS and its components that minimise the risks of untimely and incomplete identification of significant and critical failures and gaps in the ICS;

###### reporting the existing gaps of the ICS to management bodies and managers of the appropriate level responsible for corrective actions;

###### monitoring the timeliness and completeness of the elimination of identified violations, deviations and gaps in the ICS.

#### The ICS shall be monitored by:

###### the Management, Business Process Owners and employees of business units on a permanent basis;

###### Business Unit in Charge through control design performance review and ICS performance (maturity) evaluation;

###### the IAS through audits in accordance with the annual audit plan.

#### Participants of all three lines of defence of the ICS, Business Process Owners, employees, in case of detection of gaps in the ICS, KMG’s internal documents that render ineffective internal controls, shall initiate changes to KMG’s internal documents.

#### Internal control gaps identified at all levels of the lines of defence shall be reported to the heads of business units in a timely manner and promptly eliminated. Significant gaps in internal control shall be reported to the Business Unit in Charge in order to assess risks and inform KMG’s Management Board / Board of Directors.

#### ICS improvement involves:

###### elimination of all gaps identified by the IAS;

###### monitoring of the entire ICS as a whole to ensure its effective operation;

###### monitoring of best practices and international standards in the field of internal control and timely update/development of internal documents.

#### Monitoring involves the following:

###### establishment of controls at all levels of KMG management;

###### implementation of an IAS work plan for the corresponding year;

###### business process monitoring;

###### communicating the necessary information to all ICS entities.

#### For the purpose of effective and reliable operation of the ICS, KMG’s Board of Directors and KMG’s Management Board shall provide procedures for continuous monitoring and feedback to ICS entities.

## Risk Culture

#### Development of a risk culture is a necessary element of an effective ICS and gives balance to KMG’s Management and employees when making a risk/reward decision.

#### The development of a risk culture consists of: continuous training, introduction of risk management tools into everyday practices, building an incentive system that ensures the use of risk management tools, communication of values and philosophy of risk culture within KMG.

#### To improve the risk culture and awareness of KMG’s employees about the ICS, the Business Unit in Charge can annually conduct training sessions for employees of KMG and SDEs in charge of ICS area, and, if necessary, can conduct training for KMG’s Management Board and Board of Directors, ICS surveys and testing of KMG’s employees.

#### When a new employee is hired by KMG, he/she shall read and understand the Internal Control Policy and Regulations, as well as ICS onboarding materials.

#### At the discretion of the Management, employees may be rewarded for timely identification of a significant risk and its effective elimination/minimisation/management.

#### To make the employees of the Business Unit in Charge aware of the best local and international practices and improve ICS, they shall, at least once a year, undergo training/workshops, and exchange experience between the portfolio companies of Samruk-Kazyna JSC.

## ICS Performance (Maturity) Evaluation

#### Three methods shall be used for ICS performance (maturity) evaluation:

###### internal evaluation (self-evaluation) by the Business Unit in Charge;

###### internal evaluation by the IAS;

###### third-party independent evaluation by external consultants.

#### During the internal evaluation, the Business Unit in Charge shall conduct the following on a quarterly and annual basis:

###### On a quarterly basis, the Business Unit in Charge shall request information on the status of the implementation and formalisation of the ICS in KMG’s SDEs. Employees in charge of the ICS shall fill out the received questionnaire within 5 calendar days. The results obtained shall be submitted to the Risk Committee and the Audit Committee.

###### On an annual basis by 1 October, the Business Unit in Charge shall send a ready-made questionnaire with criteria to SDEs in order to obtain a more accurate and objective level of maturity at KMG and in its SDEs. Evaluation criteria shall be based on COSO methodology, international best practices, and be business-specific. SDE employees in charge of the ICS shall fill out the questionnaire and return it by 31 October. If there are concerns about the accuracy of answers, the Business Unit in Charge shall request additional clarifications. The evaluation shall be documented in a report by 30 November indicating the weaknesses/vulnerabilities of the ICS and recommendations for ICS improvement in KMG’s SDEs. The annual ICS performance (maturity) evaluation (self-evaluation) report shall be submitted to the Risk Committee and the Audit Committee for review by 31 December.

#### ICS performance (maturity) evaluation shall be performed by the IAS in accordance with the Procedure for Diagnosing Corporate Governance in Legal Entities with More Than Fifty Percent of Voting Shares Directly or Indirectly Owned by Samruk-Kazyna JSC, KMG’s internal documents in the field of risk management and internal control system performance evaluation.

#### The IAS shall prepare an IAS performance evaluation report and duly submit it to KMG’s Board of Directors for review and approval. The Audit Committee shall oversee the ICS performance evaluation and also review the report on its results. The Business Unit in Charge shall prepare an action plan for ICS nonconformity correction and improvement.

#### The third-party independent performance evaluation of the internal control system shall be performed by an external independent consultant at least once every 5 years, depending on changes in organisational activities and the overall level of maturity, reliability and performance of the ICS.

#### The third-party independent performance evaluation of ICS shall include a performance evaluation of controls, an evaluation of the level of ICS components, and a performance evaluation of controls that protect KMG’s applications and systems from cyber risks. The results of such evaluation shall be reported to KMG’s Board of Directors.

#### Based on the conclusions and recommendations derived from the third-party independent performance (maturity) evaluation of the ICS, the Business Unit in Charge shall develop a set of measures aimed at eliminating the identified gaps and increasing the level of maturity of KMG’s internal control system.

## ICS Structure and Interfaces between ICS Entities

#### The internal control system model in terms of hierarchy levels, roles and authority of the main entities of the internal control process:

Level of the Board of Directors and executive bodies

Level of Units / Business Units

Level of the Board of Directors and executive bodies and dedicated control bodies

**Level 3.**

Process controls

**Level 2.**

Corporate controls

**Level 1.**

Organisational and functional

**ICS**

###### Level 1 Organisational and Functional is associated with the organisation of the internal control system, interfaces of its participants and the tone from the top.

###### Level 2 Corporate Controls is associated with the implementation of corporate-level controls — management mechanisms that are established at the level of KMG or business units and contribute to the achievement of KMG’s goals, directly or indirectly affecting the risks inherent in its business, enabling to more effectively structure the internal control system by influencing the control environment as a whole and the performance and number of controls. Corporate-level controls have an effect on KMG as a whole, on each business process, and are associated with monitoring compliance with key features and criteria of reliability and level of maturity to which it is necessary to strive. Such features, criteria and maturity levels are defined in KMG’s policies, KMG’s long-term development program, and a number of other conceptual and regulatory documents of KMG.

###### Level 3 Process Controls is associated with the implementation of controls that are built into the business processes and day-to-day activities of employees, and do not affect the control environment of KMG as a whole.

#### The ICS organisational structure is shown in the KMG-F-3214.2-37/RG-3209.2-37 form hereto.

#### In order to better understand ICS in terms of roles and responsibilities, KMG has implemented the Three Lines of Defence Model. Each of the three lines of defence plays a special role within the broader management structure of the company. When everyone performs their role effectively, it increases the likelihood that the company will be successful in achieving its goals. The responsibilities of each of the groups (or lines) are as follows:

#### The first line of defence — business units form the first line of defence with the help of control mechanisms responsible for the implementation of risk management elements in the decision-making process and key business operations of the company. Business units are risk owners and are responsible for identifying, managing, reducing risks, analysing and reporting on key risks. The Heads of Business Units shall develop, implement and maintain controls in the supervised business processes.

#### The second line of defence — business units in charge of risk management at KMG shall develop and implement a methodological approach to risk management, define standards and coordinate the company’s risk management actions, including relevant processes, technologies and culture. The second line includes business units in charge of risk management, internal control system, security, compliance, legal support, etc. They provide continuous monitoring of the development and operation of controls related to the first line of defence, advise on risk management issues, conduct training of company employees.

#### The third line of defence shall conduct an independent quality assessment of existing risk management processes, identify violations, and make suggestions for improving the risk management system. The Board of Directors shall accept this conclusion as a guide to action. Under the supervision of the Audit Committee, the Internal Audit Service shall monitor the functions of the first and second lines of defence, and the implementation of corrective actions, to improve the risk management system. Interfaces between ICS entities in the Three Lines of Defence Model are shown in Table 6.

**Table 6. Interfaces of ICS Entities**

|  |  |  |
| --- | --- | --- |
| **1st LoD** | **2nd LoD** | **3rd LoD** |
| * Owns and manages risks; * In charge of an effective ICS and development of corrective actions for the identified gaps; * Executes controls; * Develops and implements internal documents. | * Advises on the design and implementation of controls, risk management, fraud prevention, etc.; * Defines a unified procedure for identifying, evaluating, reviewing and developing risk response measures; * Tracks the maintenance of an effective ICS, risk assessment, etc. | * Follow-up on corrective actions; * Monitoring of the functions of the 1st and 2nd LoDs; * Provides the Management and the Board of Directors with guarantees that the risk management and control efforts of both the first and second lines meet the expectations of the Board of Directors and the Management. |

## Assurance Map

#### The assurance map defines the roles and responsibilities for the effective operation of KMG’s business processes, risk management and internal control between the three lines of defence. These roles and responsibilities minimise/eliminate duplication of the functions of reviews and monitoring of risk management and internal control systems, including monitoring of action plans based on such reviews.

#### In order to develop Assurance Maps, the Business Unit in Charge shall submit current and long-term review plans for the supervised areas and draft Assurance Maps by 30 October using the KMG-F-2727.2-37/RG-3209.2-37 form. After the review of Assurance Maps by the IAS and the necessary business units, the Business Unit in Charge shall submit them to KMG’s Management Board for review and approval by 31 December. The Assurance Maps shall be updated as necessary.

# **PERFORMANCE CRITERIA**

## Performance criteria include:

###### Timely submission by Business Process Owners of information/documents on the ICS to the Business Unit in Charge, and development and/or update of risk and control matrices and flowcharts for each business process defined in the Business Process Classifier, for which it is necessary to develop and/or update risk and control matrices and flowcharts.

###### Timely submission of risk and control matrices by the Business Unit in Charge to the Risk Committee for review and to KMG’s Management Board for approval.

###### Timely control efficiency testing by the IAS.

###### Timely submission of an IAS report on ICS performance evaluation to KMG’s Board of Directors for review.

###### Timely implementation of the ICS improvement action plan.

###### Timely provision of up-to-date information by business units / the IAS.

###### Annual approval of a CLRCM by the 30th day of the month following the reporting year.

###### Timely internal performance (maturity) evaluation of the ICS by the Business Unit in Charge.

###### Timely submission by the Business Unit in Charge of the Annual ICS Performance (Maturity) Evaluation Report to the Risk Committee and the Audit Committee.

# **REFERENCES\***

|  |  |
| --- | --- |
| Approved by KMG’s Board of Directors on 12 December 2018/Minutes No. 19/2018 | Internal Control System Policy of JSC NC “KazMunayGas” |
| Approved by KMG’s Board of Directors on 8 May 2019/ Minutes No. 7/2019 | Regulations on the Audit Committee of the Board of Directors of JSC NC “KazMunayGas” |
| Approved by KMG’s Board of Directors on 10 March 2017/ Minutes No. 13 | Regulations on the Risk Committee of JSC NC “KazMunayGas” |
| Approved by the Fund’s Management Board on 26 September/Minutes No. 35/16 | Procedure for Diagnosing Corporate Governance in Legal Entities with More Than Fifty Percent of Voting Shares Directly or Indirectly Owned by Samruk-Kazyna JSC |

\* When using these Regulations, it is advisable to check the validity of the reference documents as of the current year. If a reference document has been superseded (revised), the superseded (revised) document shall apply as a reference when using these Regulations. If the reference document is cancelled without being superseded, the provision referring to it shall apply to the extent not affecting this reference.

# **RECORD FORMS**

|  |  |
| --- | --- |
| KMG-F-3210.2-37/RG-3209.2-37 | Business Process Classifier of JSC NC “KazMunayGas” |
| KMG-F-3211.2-37/RG-3209.2-37 | ICS Schedule |
| KMG-F-3212.2-37/RG-3209.2-37 | Flowchart of JSC NC “KazMunayGas” |
| KMG-F-3213.2-37/RG-3209.2-37 | Risk and Control Matrix of JSC NC “KazMunayGas” |
| KMG-F-3214.2-37/RG-3209.2-37 | ICS Organisational Structure of JSC NC “KazMunayGas” |
| KMG-F-3215.2-37/RG-3209.2-37 | Corporate-Level Risk and Control Matrix of JSC NC “KazMunayGas” |
| KMG-F-2725.2-37/RG-3209.2-37 | Control Design Review of JSC NC “KazMunayGas” |
| KMG-F-2726.2-37/RG-3209.2-37 | Control Design Review Report of JSC NC “KazMunayGas” |
| KMG-F-2727.2-37/RG-3209.2-37 | Assurance Map of JSC NC "KazMunayGas” |

# **PROCESS FLOWCHART**

| **Flowchart** | **Action** | **Timing** | **Action Owner** | **Record** |
| --- | --- | --- | --- | --- |
| **Process entry:** |  | | | |
| 1 | 1. Develop/update the business process classifier — 5.1.1–5.1.8 | By 15 October | Business Unit in Charge | Business Process Classifier |
| 2  yes  no | 2. Review and approve the developed business process classifier — 5.1.9 | By 30 November | Risk Committee, Management Board | Approved Business Process Classifier |
| 3 | 3. Prepare the ICS schedule — 5.1.10–5.1.14 | By 1 December | Business Unit in Charge | ICS Schedule |
| 4 | 4. Report on the need to develop and/or update risk and control matrices — 5.1.11 | By 15 November | Business Process Owners | Memo on the need to develop and/or update flowcharts and risk and control matrices |
| 5  yes  no | 5. Review and approve the ICS schedule — 5.1.14–5.1.16 | By 31 December | Risk Committee, Management Board | Approved ICS Schedule |
| 6 | 6. Develop and/or update flowcharts, risk and control matrices — 5.2.1–5.2.28 | By 15 November | Business Process Owners (jointly with the Risk Coordinator) | Developed and/or updated flowcharts, risk and control matrices |
| 7  no  yes | 7. Review business process flowcharts, risk and control matrices — 5.2.11, 5.2.14–5.2.15 | By 15 November | Business Unit in Charge | Reviewed flowcharts, risk and control matrices |
| no  8  yes | 8. Review and approve developed and/or updated risk and control matrices and flowcharts — 5.2.16–5.2.17 | By 31 December | Risk Committee, Management Board | Approved flowcharts, risk and control matrices |
| 9 | 9. Prepare control efficiency testing plans for business processes — 5.5.1 |  | IAS | Control Efficiency Testing Plans |
| 10 | 10. Test control efficiency for business processes — 5.5.2 |  | IAS | ICS Improvement Conclusion |
| no  11  yes | 11. Review and approve — 5.5.3 |  | Board of Directors | ICS Improvement Conclusion |
| 12 | 12. Evaluate ICS performance — 5.9.3 |  | IAS | ICS Performance Evaluation Report |
| 13  no | 13. Review and approve — 5.9.4 |  | Board of Directors | ICS Performance Evaluation Report |
| **Process exit**  yes |  | | | |