Approved

by resolution of the Board of

Directors of “Samruk-Energy” JSC

dated \_\_\_ \_\_\_\_\_\_\_\_\_\_\_ 2016

Minutes No.\_\_\_\_\_\_

**CORPORATE MANAGEMENT SYSTEM**

**Rules for assessment and identification of “Samruk-Energy” JSC risks**

**PR 03-03-10**

**Astana 2016**

**The list of amendments and additions registration**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Amend**  **ment**  **number** | **Page no.** | **Date of amendment/addition introduction** | **Inspection date** | **Signature of a responsible person** |
| **1** | **2** | **3** | **4** | **5** | **6** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Table of content**

1. [Purpose 4](#_bookmark0)
2. [Field of application 4](#_bookmark1)
3. [Definitions and abbreviations 4](#_bookmark2)
4. [Responsibility 5](#_bookmark3)
5. [Normative references …](#_bookmark4) 5
6. [General provisions 6](#_bookmark5)
7. [Risk identification](#_bookmark6) 6
8. [Risk evaluation 1](#_bookmark7)0

[FD 01 PR 03-03-10 2](#_bookmark8)3

F[Z 01 PR 03-03-10 2](#_bookmark8)5

[Annex 1 2](#_bookmark9)6

[Annex 2](#_bookmark10) 29

Annex 3......................................................................................................................................32

Annex 4 ……………………………………………………………………………………….33

# Purpose

# 1. These Rules for identification and assessment of "Samruk-Energy" JSC risks (hereinafter - Rules) are developed in accordance with the Risk Management Policy of "Samruk-Energy" JSC (hereinafter - Policy) and other internal regulations governing the activity of "Samruk-Energy" JSC (hereinafter - The Company).

# 2. The rules shall determine the order, procedures, methods of identification and assessment of risks, as well as control over current risks and monitoring the effectiveness of risk management practices. More detailed approaches to risk assessment may be set forth in documents that govern the management of the Company’s individual risks.

# 3. Identification of risks and the presence of real objective view of existing risks is one of the foundations of effective risk management, contributing to the achievement of Company goals.

# 4. Risks identification shall provide a tool for registering and notifying of possible adverse events that could adversely affect the achievement of goals and objectives set to the Company and each of its employees, as well as for determining the direction and the need to improve the risk management process.

# 2 Field of application

# 5. Observance of Rules shall be mandatory for all employees of the Company.

# 6. Employees of the Company who are representatives of the Company in the management bodies of subsidiaries (hereinafter - SA) must ensure the compliance with requirements set out in this Rules.

# 7. The Company’s SA shall develop their own rules for risks identification and assessment.

# 3 Definitions and abbreviations

# 8. The following definitions and abbreviations shall be used in the Rules:

1) Risk Register - is a list of risks faced by the Company in its activities, which also includes various scenarios of possible risk occurrence. Risk owners shall be identified for each risk, i.e. business units that deal with this risk by virtue of their duties. At the same time, the consolidated risk register of Company’s group shall include only critical risks of SA which are in the red zone of SA Risk map.

# 2) Risk Map - is graphic and text description of limited number of the Company's risks, located in a rectangular table, at one "axis" which shows the force of impact or significance of risk, and at the other the likelihood or frequency of its occurrence. Horizontal axis on the map shows the probability or frequency, and the vertical axis shows the force of impact or significance. In this case, the probability of risk emergence increases in moving from left to right on the horizontal axis and the impact of the risk increases from bottom to the top on the vertical axis increases below the top of the vertical axis;

# 3) The probability of risk occurrence – risk occurrence frequency

# 4) Impact - the value of potential loss that could arise in the risk occurrence

# 5) Impact time - the duration of the risk impact

# 6) Risk assessment period - the date as of the end of the reporting period.

# 7) Inherent risk - this is the amount of risk that is present in the absence of actions on the part of risk owners to change the likelihood or degree of impact of this risk on the achievement of the objectives of the Company;

# 8) Residual risk – the risk that remains after taking action by risk owners to change the probability of risk or degree of impact of this risk.

# 9) The amount of loss - the amount of the forecasted loss due to risk occurrence.

# 10) The Fund - Sovereign Wealth Fund "Samruk-Kazyna" JSC

# Other terms used in the Rules shall have the meanings set by the Risk Management Policy of the Company.

# 4 Responsibility

9. The business unit of the Company in charge of risk management shall be responsible for organization of risk assessment

10. The business unit of the Company responsible for risk management shall coordinate the work with all departments of the Company. The annual survey, in accordance with Annexes 2 and 3 of the Rules that is carried out by Company’s risk management business unit as well as inquires on key risks including Reports on execution of the Action Plan for key risks management according to FZ01PR03-03-10 shall be mandatory for all units and personnel of the Company.

11. The Company’s risk management unit shall provide support to business units of the Company’s SA responsible for risk management during the identification and assessment of risks, and also shall carry out risks consolidation across the Company group.

12. The Company’s risk management unit shall report to the officer who is in charge of risk management in the Company (risk officer) on the matters related to risk assessment and identification.

# 5 Normative references

# 18. The Rules are designed to meet requirements of the legislation of the Republic of Kazakhstan and the following internal documents of the Company (but not limited to):

# 1) The Company’s Charter;

# 2) Risk Management Policy of the Company;

# 3) Rules for identification and assessment of Fund’s risks;

# 4) Rules for internal regulatory documents management

# General provisions

# 19.Each employee of the Company shall express his view on the available risk in the questionnaires according to Appendix 3 of the Rules on a yearly basis or during other events aimed at identification and assessment of the Company’s risks that are held by the Company’s risk management division

# 20. The risk register shall be generated on the basis of identified events; this Risk Register represents systematic list of all risks which the Company faces.

# 21. The Company shall conduct the work on consolidation of risks of the Company group as well as evaluation of their effect on the consolidated financial position of the Company, including on the basis of annual consolidated information according to the form FD01 PR03-03-10 (Risk Register) to the Rules and paragraph 65 of Rules (Risks Map) presented in the framework of submitting the matters for consideration of the Company’s SA management bodies not later than 1 October preceding the forecast period.

# 22.Risk management division shall on an annual basis before 1 November of the year preceding the forecast period, provide the Board of Directors with consolidated risk register of the Company according to the form presented in the FD 01PR 03-03-10 (Risk Register) to the Rules and paragraph 65 of the Rules (Risk Map)

# 7 Risk Identification

# 23. Risk identification is important as a method of optimizing the Company’s costs, since the early identification of risks, determination of appropriate measures for their mitigation and elimination of consequences allows planning the sources and amounts of financing such activities, which ultimately influence the efficiency of the Company's operations. A combination of different techniques and tools shall be used to identify risk. Events shall be identified from the perspective of both past experience and possible future events. The main methods are described below.

# 24. Risks can be identified using two approaches:

# 1) Initial identification and risks inventory - initial preparation of the Company’s Risk register in the implementation of the risk management system and its regular revision;

# The Company's risk register shall be drawn up during the initial risk identification,

# in order to carry out the subsequent evaluation and determine the approaches to managing these risks. The process of risk inventory involves regular (not less than once a year) revision of previously identified risks, i.e. determining the relevance and materiality of risks that are in the Company’s risk register. Some of the previously identified risks may be deemed irrelevant as a result of inventory.

# 2) Detection of potential risk - identifying potential risk in the normal course of business.

# New risks can be found not only in the course of conducting regular procedures within the framework of risk management system but also in the performance of current activities by the Company group’s employees.

# In the event of revealing information about potential risks that were not previously included in the register, an employee of the business unit must send a relevant service note which outlines the information and assumed consequences of risk event occurrence to the risk management division. Risk management department shall analyze, evaluate the received information and if necessary include to the new risk register of the Company.

25.**Identification of risks on the basis of set goals and objectives**: potential events that may affect the achievement of goals shall be determined on the basis of set goals or well- balanced indicators system. Events shall be identified by risk owners and approved by risk management division, and the risk register shall be compiled on this basis; risk register – a list of risks inherent to the company and (or) related to it its activity.

26. **Industry and international comparisons**: Risk Register shall be compiled on the basis of a list of potential events inherent to organizations such as the Company and (or) organizations according to industrial specialization or functional activity

27. **Seminars and discussions:** Risk Register shall be compiled on the basis of arranged discussions (brainstorming, round table, etc.) with the Company's employees about potential events that may affect the organization and the achievement of its objectives. Such discussions may be held in every business unit for determining the events (risks) that influence the activity of every such business unit and the Company group as a whole, the results shall be then integrated in a common risk register (or the current Risk Register shall be complemented/corrected)

**28. Interviewing:** The business unit of the Company responsible for risk management, shall conduct target interviews with key employees (experts) of the Company for an open discussion of existing and potential risks and ways to manage them. Typically, these interviews are conducted with the heads of structural divisions of the Company.

**29. Monitoring publications and presentations**. In order to identify risks, the Company publications, speeches by executives of industry-specific ministries and organizations, opinions of industry experts are monitored on a regular basis, as well as drafts regulatory-legal documents, concepts of the industry development , analysts' forecasts, materials of specialized conferences are analyzed.

**30. Analysis of reports on results of the audit and other inspections**. This method shall represent an inspection of individual areas of the Company group’s activity and can be combined with carrying out certain expert methods (surveys, interviews). The compliance of available documentation with the actual practice of applying regulations shall be checked; the regulatory framework and guidelines shall be analyzed. As a result the conclusion shall be prepared, on the basis of which risks will be identified.

**31. Near Miss analysis** is to register all violations (operational, production and so on.) of regulations and forecasting the probability of risk events occurrences on the basis of these violations. At this, because of uncertain factors, violation of regulations may not lead to the immediate occurrence of risk event, but the probability of occurrence of this risk event is much higher and unexpected if there are more facts when the risk event failed to occur

Near Miss is an incident which under certain circumstances could lead to injury, fire, flood, accident, etc., but did not lead. Statistics show that for every 600 Near Miss there is a high probability of occurrence of a significant incident - the implementation of a risk event

1. **Database of losses occurred**: The Company shall constantly monitor occurred losses; information on which will help to identify events that have a negative effect on the Company’s performance. In addition, database of losses occurred is a good basis for quantitative assessment of risks. The database shall be based on reports of Company’s business units and may also include data from external sources. This method shall comprise:
2. Analysis of data on violations - the analysis of the registered violations, emergency situations, failures in the processes of the Company and other facts of deviations of current activity indicators from the planned.
3. Analysis of reports – analysis of reports and other documentation of the Company, including management, accounting, tax reporting, the Company's performance indicators, plans, registers and contracts, etc.
4. Analysis of experience of other companies – a comparative analysis of the Company’s processes and performance with other large companies. Periodicals and reports of specialized agencies may be used for analysis.
5. Identified events and risks shall be systematized in the form of risk register in accordance with table No. 2 of these Rules. The form and level of specification of risk register may be changed with the development of the risk management system. Grouping of risks may be effected on the assumption of risk nature, their interconnection as well as other factors (e.g., the use of certain risk management methods)
6. Company’s risk register is a list of risks faced by the Company in its operations, distributed in four major categories of risk, which also includes various scenarios of of possible risk occurrence. Risk owners shall be identified for each risk.
7. The risk register shall comprise 4 parts:

1) Risk passport which indicates the KPI, its threshold value, the name of the risk that could hinder the achievement of KPI, the cause of the risk, a description of possible consequences of risk occurrence , a key risk indicator and risk owner.

2) Assessment of inherent risk – the risk assessment in regard to impact, probability and the period of risk impact shall be carried out in this part. Calculation of points of significance shall be made pursuant to paragraph 60 hereof.

3) Risk management measures – risk management activities including current and scheduled shall be described in this part.

4) Risk assessment as a result of activities implementation – the risks shall be evaluated following the implementation of activities. This part of register allows evaluating the efficiency of activities aimed at risk management.

36. Systematization of the identified risks allows:

1)achieving consistency in the classification and quantitative evaluation of risks, which helps to improve the comparison of risk profile across the Company group (for business processes, departments, projects, etc.);

2) providing a platform for building more complicated tools and quantitative risk assessment techniques;

3) providing an opportunity for coordinated risk management and control both in the Company and subsidiaries.

37.In order to standardize risk register and consolidate risks into the Company’s single risk map, the Company group shall use a single classification on designation of main risks described in Annex 1 to the Rules

38. The following format shall be used to identify the range of risk: "Number of risk" - "Risk category" - "Short name of the company" For example, for currency risk of the Company, according to the mentioned format it will be: “5-F-SE which means a risk No. "5" ,category "financial" , risk owner is "Samruk-Energy".

1. Subsidiaries of the Company shall use the classification of risks contained in Annex 1 of these Rules in order to designate SA risks, in order to consolidate the critical risks of the Company’s SA into risk register of the Company group.
2. If the risk specific to SA is not available in the range of risks, then SA shall mark this risk by adhering to the above format using the continuing number (digital numbers in risks numbers specified in the range of risks may not be used for marking other risks).
3. The main result of this stage of risk management system shall be the formation of a consolidated risk register of the Company group. At this, only critical risks of SA which are in the red zone of SA risks map shall be included in the consolidated risk register and risk map of the Company group. Thus, the identification of subsidiaries critical risks shall be conducted on the basis of inherent risk evaluation.
4. Critical risks of the Company’s subsidiaries should be included in the corresponding area of ​​risk maps, in accordance with the magnitude of the potential damage caused by the implementation of a risk event, which shall be determined on the basis of consolidated risk appetite of the Company. Thus, the risks which are in the red zones of SA risk maps can be attributed to the green zone on the risk map of the Company. Risks which are in green and yellow zones of SA risk maps shall not be included in the risk register of the Company since these risks shall be managed independently, at the level of subsidiaries.
5. Risk Register shall be revised, clarified or complemented on an annual basis or more frequently as information about risks becomes available; the information shall be submitted to the Company’s business unit responsible for risk management by business units of the Company during identification of new or changing the status of existing risks. At including a new risk to the risk register or changing the status of existing risk with potential impact higher than the risk appetite and a high probability of its occurrence, a business unit of the Company responsible for risk management shall communicate to the Board of Directors such risks with proposals to minimize them
6. The risk management business unit shall be in charge of carrying out activities on identifying of risks and formation of risk register, including consolidated.

Risk Register shall be subject to agreement with risk owners.

1. Due to the reason that activity of SA are multidirectional, strategic and legal risks may not be aggregated for the group of the Company, but may be combined depending on the belonging to a particular industry or direction. Financial risks shall be provided on an aggregated basis in the Company’s risk register. The Company (Head office) risks shall be marked out separately.
2. The Company’s business units shall be responsible for providing the Company’s risk management division with information about risks, including critical risks of SA
3. The process of identifying operational risks shall be carried out within the framework of the identification and assessment of risks on a continuous basis in accordance with these Rules and other internal documents of the Company.
4. Depending on circumstances (reasons) of operational risk occurrence, events or incidents of operational risks shall be classified according to risk factors as follows:

1) external fraud - robbery, forgery of documents, theft of documents / information, hacking / cracking of information systems and other cases that occurred through the fault of third parties;

2) internal fraud - cases of losses occurrence due to willful misconduct of the Company personnel, including abuse of official capacity, intentional concealment of transactions, information leakage, theft, fraud, extortion, embezzlement of material assets, misappropriation or willful damage to the Company's property;

3) labor relations - cases of labor disputes with employees, violation of labor laws, including health and safety requirements, high staff turnover, disclosure of confidential information by employees, the lack of professional skills of the staff;

4) customers and business practices – cases of legislation violation during the performance of core activity; failure or improper fulfillment of obligations to customers, contractors and other third parties arising from contracts relating to the main activity, violation of business practice;

# 1) Failure in the information and technology systems - cases of

# failure of equipment and systems, and as a consequence, the loss of information data, untimely submission of reports to supervisory bodies and so on;

# 2) process management - inadequate organization of internal processes and procedures, violations of established limits, the lack of protection system and the procedure for access to information, poor organization of information flows within the Company, errors in data entry and treatment of data on operations and transactions and so on;

# 3) damage to physical assets - the loss of or damage to property, equipment and other tangible assets as a result of objective situations beyond the control of the Company (man-made);

# 4) industrial accidents - events causing damage to health and life of employees who are in the process of execution of functional duties.

# 49. The list of indicators shall be provided in Annex 4 to the Rules, which may be amended or supplemented as various cases of operational risk arise.

# 8 Risk evaluation

# 50. Risk assessment allows the Company to analyze the impact of the potential risk to the achievement of its objectives. Risks shall be assessed in terms of probability or frequency of occurrence and the impact, if possible using a combination of qualitative and quantitative methods. Positive or negative impact of potential risks should be evaluated individually or in conjunction with the whole organization that is in the Company Group. Risks shall be assessed in terms of their full impact (gross risks).

# 51. The risk assessment process shall be carried out to identify the most significant risks that could adversely affect the Company Group's operations and achievement of its strategic goals and objectives. These risks shall be submitted for consideration of the Board of Directors and decisions on their management and control shall be taken.

# 52. Initially, the risk assessment shall be carried out on a qualitative basis, then for the most significant risks the Company should carry out quantitative risk assessment using the following approaches to evaluation depending on the particular situation.

Thus, in the evaluation of technological risks it is necessary to conduct the risk estimation on the basis of property value, on the basis of shortcoming in revenue and etc. Risks shall be assessed only on qualitative basis if they do not fall for a quantitative assessment or reliable statistical information for modeling is not available or building such models is not feasible in terms of expenses,

# 53. Quantitative evaluation shall allow receiving more accurate analytical data, and is particularly useful in developing methods for risk financing.

# 54. At the stage of preparation of the qualitative risk assessment, the basic parameters of such assessment shall be established. The risk assessment shall be carried out on the basis of three indicators - the frequency or probability of risk; the period of influence and a risk size.

# A point scale shall be introduced to ensure comparability between risks and facilitate a qualitative evaluation:

# Frequency or probability of a risk

|  |  |  |
| --- | --- | --- |
| **point** | **meaning** | **Frequency or probability** |
| **1** | Very rare | Once in 7 or more years (or the probability of occurrence up to 5%) |
| **2** | rare | Once in 5 years (or the probability of occurrence 25%) |
| **3** | From time to time | Once in 3 years (or the probability of occurrence 40%) |
| **4** | Often | Once in a year (or the probability of occurrence 80%) |
| **5** | Very often | Once in a half year or even often (or the probability of occurrence higher than 95%) |

**Risk influence period**

|  |  |
| --- | --- |
| **point** | **Influence period** |
| **1** | time for correction is available |
| **2** | risk influence shows up with time lag |
| **3** | Risk appears with immediate effect |

# 55.Assessment of risk impact shall be carried out in monetary terms on the basis of consolidated risk appetite of the Company as defined in Policy. For the purpose of reporting to the Company and for the consolidation of subsidiaries and affiliates’ critical risks in a single risk register and the map of the Company, SA shall use the assessment of the impact of SA critical risks according to the following table.

**Risk size (financial indicators)**

|  |  |  |
| --- | --- | --- |
| **point** | meaning | **Potential loss from the risk occurence** |
| 1 | Insignificant | Less than 25% of the risk-appetite level |
| 2 | obvious | 25-50% of the risk-appetite level |
| 3 | significant | 50-75% of the risk-appetite level |
| 4 | critical | from 75% of the risk-appetite level up to risk-appetite value |
| 5 | disastrous | Higher of the risk-appetite level |

56. When submitting a quarterly information on the risk map of SA , SA in addition to SA risk map shall provide a separate risk map indicating SA’s critical risks on a consolidated risk map of the Company according to the impact of risk on the consolidated risk appetite of the Company.

# Transition to the quantitative risk assessment on the basis of indicator of cash flow exposed to risks (Cash Flow at Risk) will be carried out after the introduction of risk-oriented financial model in the Company. The potential damage from the risk occurrence will be calculated on the basis of historical data from the database of occurred risks, using the Monte Carlo simulation.

# Characteristics shall be introduced for risks the impact of which is difficult to assess in financial values (such as personnel risks, reputation and etc); those characteristics shall show the risk size in comparable points. Non-financial indicators of the risk importance may be determined on the basis of balanced indicators on the basis of significance of deviations from the objectives.

**Non-financial indicators of risk influence**

|  |  |  |
| --- | --- | --- |
| **point** | **Influence degree** | **Potential loss from risk occurrence** |
| **1** | insignificant | The absence of any consequences in case of risk occurrence |
| **2** | low | Consequences of risk occurrence are insignificant |
| **3** | average | Consequences of risk occurrence are insignificant and may be fully corrected |
| **4** | material | Consequences of risk occurrence are very significant, but may  be corrected to a certain extent |
| **5** | catastrophic | In case of risk occurrence, the company may not recover from the consequences associated with this risk  recover from the impacts of this risk |

1. Risk Register and the point scale of risk assessment by frequency (probability), influence period and risk size (influence) shall be communicated to key employees (experts) of the Company to conduct qualitative assessment of risks.
2. Qualitative assessment of risks shall be carried out either by target interviewing of key personnel, or by means of questionnaires at which experts are invited to choose risks that they find most important for organizations, to evaluate them on the proposed point scale, as well as give suggestions (recommendations) to manage them. A combination of both methods may be used: a broad survey of employees of the Company on the basis of the electronic system of questioning and interviewing of business units heads, executive and managing directors of the Company, except for members of the Management Board.
3. When carrying out an expert risk assessment, experts must apply the net assessment only on the condition that the current activities are estimated by experts as effective. At this, assessment of the effectiveness of activities should be confirmed. Otherwise, the risk assessment shall be carried out on an inherent basis.
4. Obtained results shall be processed: risk indicators for each risk shall be calculated on the basis of the aggregate assessment of experts, risks shall be assigned significance ration and a risk map shall be created on this basis.
5. The point shall be calculated as follows:

**Significance point = (frequency + occurrence time ) \* impact**

1. For operational risk assessment, the value of operational risk rating (RR) of each type of risk according to below table shall be determined on the basis of Risk significance point:

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk significance point** | **Risk rating value, RR** | **General significance of the risk** | **Specification** |
| **from 28,1 to 40** | 1,00 | Extremely high | Risk response actions must be determined or if they are available, must be improved, prepared for execution before the implementation of the project/task or during the project/task implementation stage immediately after detection of the risk |
| **from 15,01 to 28** | 0,9 | high | Risk response actions must be determined or if they are available, must be improved and executed within 1 month during the project/task implementation. |
| **from 8,01 to 15** | 0,8 | average | Risk response actions must be determined or if they are available, must be improved within 3 months as well as executed during the project/task implementation. |
| **from 1,01 to 8** | 0,6 | low | The risks of this category should be monitored, but the preparation of response actions is not required. |
| **from 0 to1** | 0,5 | Very low |

1. Risk map allows estimating the relative importance of each risk (compared with other risks), as well as detecting risks that are critical and require development of actions for their management.

Forming of risk maps will enable to:

1) Determine the potential of risk retention to the extent that can be applied to all operations of the Company;

2) develop a list of critical risks of the Company and to ensure the availability of appropriate processes for their management;

3) to prioritize risks and develop the allocation of financial resources.

b. Risk map is divided into several areas identified by different colors.

1) Red Zone - risks that are critical to the Company either in connection with a high probability of occurrence, or due to serious potential of damage that could affect the Company’s financial stability.

# 1) Orange Zone - risks that have a high probability of occurrence or a large potential of impact on the Company's financial stability.

# 2) Yellow zone - risks that have a medium probability of occurrence or the average potential impact on the financial stability of the Company.

# 3) Green zone - risks that have a low probability of occurrence and (or) do not have a significant impact on the Company’s financial stability

5

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

4

Impact

3

2

1

1 2 3 4 5

Probability

1. Card identification numbers (in accordance with the risk register) in compliance with indices (probability) of occurrence frequency and the size of (the impact of) risk shall be entered on the map.
2. Risk map shall represent a graphical image of the Company's exposure to critical risks and shall be a must-have appendix to risk management reports submitted to the Board of Directors.
3. Priority of risks shall be established in accordance with the position of each of the risks on the risk map:

1) Group 1 - catastrophic and critical risks -red zone of risk map - risks that have the highest priority. Such risks which make up 75% or higher of risk appetite level, as well as exceed the risk-appetite;

2) Group 2 - large risks - the orange zone of ​risk map - second in terms of priority, the damage from their occurrence remains in the range of 50 - 75% of risk- appetite level;

3) Group 3 - medium risks - yellow zone of risk map - the third in terms of priority ,the damage from their occurrence remains within 25-50% of the risk –appetite level;

4) Group 4 - low risks - green zone of risk map – risks within 25% of risk- appetite level - monitoring and control.

70. For the purposes of reporting on risk maps of the Company, SA of the Company shall use consolidated indicator of the Company’s risk-appetite for evaluation of the risk impact and showing critical risks of SA on the consolidated risk map of the Company.

71. Within each of the groups the priority of a risk shall be set on the basis of risk significance score

1. Each of risks included in the 1, 2 and 3 priority group shall be evaluated on the basis of following factors:

1) analysis of risk occurrence reasons (loss scenarios);

2) analysis of potential impact of risk on the financial performance of the Company - Gross (excluding risk management techniques) and net (remaining risk after application of risk management methods);

3) analysis of risks correlation with other risks (clearing off a negative effect from the risk occurrence in one business unit by a positive in other business unit - the principle of compensation, or the strengthening of the negative effect due to occurrence of other risks - the principle of dominoes).

1. The size of the critical risk effect needs to be quantified. If it is impossible or not practical to quantify, a detailed risk assessment using a combination of qualitative assessment methods will be needed in order to achieve the highest validated assessment. At a quantitative assessment the risk is always evaluated first on gross basis, and then on net basis taking into account risk management measures. The change of a risk on a map can be shown by moving the corresponding identification number.
2. Quantitatively the risk shall be assessed on the basis of indicator of the maximum possible damage from the occurrence of each certain risk. Different methods and models can be used for a quantitative assessment.
3. Risk assessment methods shall include:

1) a quantitative assessment of risk based on the value of the property which may be damaged as a result of the risk occurrence. In such a model, scenarios of material damage at the risk occurrence shall be built, and recoverable amount of property which may be damaged and may be subsequently repaired or replaced shall be calculated. Typically it is used for quantitative assessment of operational risks (material damage to property caused by man-made disasters, fire, etc.).

2) a quantitative assessment based on the calculation of unearned income. The duration of a possible production downtime as a result of the risk occurrence shall be estimated and the income (or fixed costs) per day shall be calculated. As the result of multiplying these figures a quantitative risk assessment shall be obtained. Such an assessment is commonly used to assess the risk of production interruption or supply disruption.

3) quantitative risk assessment on the basis of comparative analysis. Evaluation of the maximum damage from some types of risks, such as risks of liability for injury or environmental pollution, cannot be calculated by any formulas and therefore case statistics shall be used for quantitative assessment of such risks

It is calculated for any formulas, and therefore to quantify these risks using case-statistics (industry and territorial).

# To assess these risks, usually scenarios of their occurrence and the parties which may be involved (suffer damage), as well as the overall impact of such risk are evaluated, and on the basis of existing information (statistics) on the cost of damage caused by occurrence of such scenario the maximum possible damage shall be determined. Case statistics is also used to assess the impact of any risks on the market value of shares and other securities of the company.

4) The quantitative risk assessment based on statistical models. This assessment shall be applied to risks that have a specific monetary value and dependence on certain external factors (e.g. oil price fluctuations, currency fluctuations, inflation expectations, etc.) and are based on the construction of statistical relationships (for example, using the methods of regression analysis). In this case, you it can be clearly identified the conditions under which the occurred risk can be significant for the Company.

76. The statistical approach is based on historical data of occurred risk events. In this approach, a quantitative risk assessment shall be carried out on the basis of an accumulated internal or external statistics. The main methods of risk assessment in the framework of this approach:

1) Value at risk - VaR - the maximum reduction in the value of the investment at a certain planning horizon (e.g., month) which will not be exceeded with a high (in advance specified) probability (typically 95% - VaR95% or 99% - VaR99%). The value of VaR has a monetary value.

2) Cash-flow at risk - CFaR - the maximum reduction in the amount of cash proceeds (or a maximum increase in costs) caused by influence of one or more risk factors

risk that will not be exceeded with a big (predetermined) probability (Usually 95% or 99%) at a certain planning horizon. The method reflects the specific risks of non-financial companies.

Due to the fact that most of assets of non-financial companies are illiquid, for them the main risk is a decline in operating cash flow. Therefore, a key value metric of a risk is cash flow at risk. In this connection it is necessary to build a model that describes the influence of one or a group of factors on the amount of cash proceeds (expenses) of the Company. Risk factors may act as market value (prices, exchange rates, interest rates), and random events (credit, operational, regulatory, etc.). Possible changes in the risk factors and the likelihood of such changes are estimated based on historical data or expert opinion. On the basis of the built model possible changes in the factors shall be transformed into possible changes in cash flow and probability distribution of cash flow changes shall be built.

CFaR method can be applied when assessing the risk of changes in cash flow for the individual type of the Company’s activity or for the Company as a whole. CFaR value shows greatest changes in the cash flows at a certain planning horizon while retaining at the entire horizon all probable spreading of risk factors and patterns of influence of these factors on the formation of the cash flows.

1) Earnings-at risk - EaR - this method of quantitative calculation of risks is an analogue of CFaR, but takes into account the accounting aspects of the Company's revenue recognition. One of the major differences between CFaR and EaR Cost is cost metric of a risk. Unlike CFaR where the cost metric of risk is cash flows, in calculating EaR, cost metric of a risk is the future earnings of the Company.

2) a quantitative risk assessment on the basis of stochastic (probabilistic Monte Carlo method) models. This assessment is used in the risk assessment, which can be expressed in monetary terms, but the correlation dependence from external factors is rather difficult to establish because the risk has a clear probabilistic nature. Such risks, for example, may include the risk of natural disasters.

At this approach different scenarios of risk events occurrence are designed, and the impact of risk events consequences on the planned cash flows, financial and economic performance of the Company are analyzed.

77. The main methods of risk assessment in the framework of stochastic (probabilistic) models:

1) Stress testing. The method helps to identify losses which the Company may incur in the occurrence of unexpected adverse events. Stress testing does not output quantitative value of risk. This method allows assessing the consequences of occurrence of various adverse scenarios and "safety reserve" of the Company in relation to risk factors. Since scenarios considered in the framework of this method are the occurrence of rare events, in stress testing any probabilities are not ascribed to them. Stress testing consists of two phases:

a) building of model of the impact of risk factors on the company’s cash flows (similar to CFaR method);

b) Development of scenarios of risk factors occurrence.

A segment of the company’s cash flows that will be involved in stress-testing should be highlighted for building a model (the most effective is the analysis of all cash flows, however, cash flows on separate financial instruments, or certain type of activities can be considered). Then it is required to identify risk factors that affect the value of the selected cash flows.

1. Dependence between risk factors effects and cash flow shall form the required model. It can be very simple for a single financial instrument (e.g. a loan with floating interest rate - the amount of each payment depends from changing the rate in a in a certain and obvious way), but correlations can be complicated for each cash flow of the company as a whole.

After creating a model, it is necessary to do the following:

1) Enter several stress scenarios into the model;

2) Assess changes in the cash flows if risk factors (parameters) that are included in scenario changes;

3) Select those scenarios for which the changes in cash flows fall outside a given criterion of materiality.

4) To analyze possible ways of reducing exposure to the risks involved in it.

Two types of scenarios shall be used in stress testing:

1. 1) One-factor scenarios - the impact of only one risk factor is considered, for example, a strong change in the price of certain services, the exchange rate, a particular counterparty default, etc. This method is interesting only to assess the "safety reserve" of the company in relation to one of those events. The larger the amount of change in the risk factor that does not lead to a significant change in cash flow, the smaller the company is exposed to this type of risk;
2. 2) Multifactorial scenarios - the simultaneous change of several factors, which is more likely in practice.
3. Stress testing can be conducted by:
4. 1) historical scenarios - on the basis of replay of events that occurred in the past. For example, the same changes in factors (exchange rates, interest rates, etc.) and the same events (default) which were at the time of any selected financial crisis are considered.

2) what-if scenarios – allows moving beyond historical events. These scenarios require the work of experts. Especially it is necessary to consider the worst scenarios (all considered factors assume the worst value that has been ever observed), and scenarios with the worst correlations.

3) Monte Carlo simulation. This method involves the implementation of a large number of tests - one-time simulations of situations development in the markets. To generate random numbers, expected (average) value and standard deviation (σ) of various parameters’ historical values are taken. As a result of these tests, distribution of possible financial results will be received , on the basis of which, by cutting off the worst according to the chosen confidential probability, Var or CFaR – assessment may be obtained. The amount of VaR shall be estimated in the following sequence:

1) the expected (average) value and standard deviation (σ) of each parameter shall be evaluated;

2) Random values ​​for each parameter within the given average value and standard deviation shall be produced, thus each time different results are obtained;

3) The amount of loss (price change) corresponding to a given probability shall be determined .

The application of these methods of risk assessment and forecasting will be possible

with the introduction of financial and economic model in the Company

78. Often for a reliable quantitative risk assessment it is necessary to apply a combination of some or all of the above methods, or specially developed methods. Mathematical models may be created for many risks, which will enable to get evaluation of their quantitative influence depending on various factors, and allow "replaying scenarios" of risk occurrence.

79. Quantitative risk assessment is needed to understand the importance of each certain risk, to assess the cost-effectiveness of managing such risks, as well as to establish parameters (terms) of contracts in transferring risk to third parties. The degree of accuracy of quantitative assessment shall be determined by the Company’s needs, but in any case, such an assessment would only give guidance to the Company, i.e. so-called "corridor". The objective of the Company in conducting quantitative risk assessment is to ensure that the "corridor" was not only wide enough to fit all the possible consequences in terms of value within its limits, but narrow enough to avoid paying excessive amounts for the transfer of risk.

80. Quantitative risk assessment allows conducting the stress analysis of the company’s financial performance exposure to risk - in terms of profitability, long-term financial stability (capitalization) and liquidity. If potential impact of risk falls outside the risk appetite limits of the Company, the risk shall relate to critical risks.

81. Operational risk assessment involves assessing the probability of occurrence of events that are the cause of operational risks occurrence, and assessment of risk impact on the Company’s operations. Operational risk assessment shall be carried out from two perspectives - qualitative and quantitative.

1) Quantitative risk assessment has probabilistic (predictive) character, and the calculation is based on statistical methods;

2) The qualitative method is used for objects and categories of operational risk, the level of which cannot be explicitly expressed in some number characterizing the possible level of losses.

e. To determine the level of operational risk the Company’s risk management division

may use the following methods:

1. statistical analysis of the sources of operational risk and actual losses;
2. point-weight method

# 82. The method based on the use of statistical analysis of operational risk sources allows making forecast of potential operating losses based on the size of operating losses that occurred in the Company in the past. When using this method, the information collected in the analytical database of events related to operational risk shall be used as basic data.

# 83. To build mathematical models of quantitative assessment of operational risks, statistical database on the events related to operational risk management at least over 5 years of Company’s operations shall be required. Until then risk management division of the Company shall carry out quantitative assessment of operational risk based on the calculation of the probability of losses from operational risks, relying on the number of cases related to operational risks, and the number of cases of operational risks occurrence.

# 84. Business units of the Company shall carry out a review of operational risks annually in the framework of risk identification process.

# 85. Further information from the Company’s business unit responsible for risk management, may be obtained in the form of answers to specific requests or in the form of reports developed for analysis of a particular event associated with the operational risk.

# 86. Each subtype of operational risk corresponding to classification of the Company’s operational risk is assigned weight ratio (WR), depending on the degree of influence on the gross income of the Company.

# The distribution of weight ratios for indicators that characterize the operational risk factors are presented in the table below.

|  |  |
| --- | --- |
| **Operational risk factors** | **Weight ratio** |
| Internal and external fraud | 0,05 |
| Labor relations | 0,10 |
| Customers and business practice | 0,10 |
| Failure in the informational and technical systems | 0,10 |
| Processes management | 0,20 |
| damage to tangible assets | 0,10 |
| Industrial accidents | 0,35 |
| **total:** | **1,00** |

83. Coefficient of operation risk (Cor) shall be calculated on the basis of data on the value of risk rating and weighting ratio of each subtype of operational risk; it will be used for further calculations. The coefficient shall be determined as the sum of productions of risk rating value of each subtype and corresponding weight ratio of operational risk factor.

Cor = Σ (WRi \* RRi), i = 1, n, where

n - total number of operational risk factors

84. Calculation of operational risk shall be carried out using the following formula:

OR= Cor \* GI \* 15%, where:

OR – quantitative assessment of operational risk,

Cor - Coefficient of operational risk,

GI - The average value of gross income for the last three years shall be calculated as the relation of annual gross income for the last three years in each of which the Company received net income by number of years in which the Company received net income. Unless the term of activity of the Company is less than three years, the average value of annual gross income shall be calculated based on the actual number of past years of activity.

The annual gross income shall be determined as the sum of the annual net income before tax, the annual amount of appropriations for the provisioning (Reserves) and the size of the incurred extraordinary expenses net of extraordinary income of the Company.

89.Received quantitative assessment of operational risks shall be used to analyze the dynamics of the strengths and weaknesses in the management of operational risks.

90. Standard values ​​for assessment of operational risk can be determined as statistical data accumulates.

91. Monitoring of operational risk shall be conducted by risk management division of the Company by regular analysis of information from the Register of risks and information

provided by the Company’s business units.

92. Minimization of operational risk involves carrying out a set of measures aimed at reducing the probability of occurrence of events or circumstances that give rise to operating losses and the level of their impact on the Company’s operations.

93. The basic methods of minimizing operational risks are the optimization of the organizational structure and business - processes, development of internal rules and procedures of current activities implementation in such a manner that to eliminate the possibility of operational risk factors occurrence.

94. Reducing the financial consequences of operational risk shall be possible through insurance. Insurance coverage across the Company shall be carried out according to the Rules for arranging insurance coverage in the Company.

95. Conducted risk assessment allows clarifying the risk map and risk importance indicators, and critical risks of the Company shall be determined on this basis. The Company must pay special attention to these risks and decisions for their management must be made immediately.

96. The main result of this risk management system stage is a list of critical risks of the Company which are brought to the attention of the Board of Directors of the Company.

**9. Document forms**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | Record name | **Record form** | **Drafted by** | **Storage place** | **Storage period** |
| 1 | Risk Register | FD 01 PR 03-03-10 | Risk owners | Business unit responsible for risk management | regularly |
| 2 | The report on implementation of Action plan for key risks management | FZ 01 PR 03-03  -10 | Risk owners | Business unit responsible for risk management | regularly |

FD 01 PR 03-03-10 **Risk register**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Risk passport(1)** | | | | | | | | | **Assessment of inherent risk (2)** | | | | |
|  |  |  | **RISK code** |  | | **Risk factors (reasons of risk occurrence)** | **Description of possible consequences from risk occurrence** | **Key risk indicator** | **Risk owner** | **probability** | **Damage size** | | **Period of influence** | **Significance point** |
| **№** | **KPI** | **Threshold value of KPI**  **(tolerance)** | **Significant risks of failure to achieve the value of strategic KPI** | | **influence** | **The amount of damage in thous. tenge** |
|  | **1** | **2** | **3** | **4** | | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** |
|  | ***STRATEGIC RISKS (risks associated with the Company’s strategy)*** | | | | | | | | | | | | | |
|  |  |  | Risk1 | |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Risk 2 | |  |  |  |  |  |  |  |  |  |  |
|  |  |  | Risk N | |  |  |  |  |  |  |  |  |  |  |
|  |  |  | … | |  |  |  |  |  |  |  |  |  |  |
|  | ***Financial risks (risks associated with financial activity)*** | | | | | | | | | | | | | |
|  |  |  | Risk N | |  |  |  |  |  |  |  |  |  |  |
|  | ***OPERATIONAL RISKS*** | | | | | | | | | | | | | |
|  |  |  | Risk N | |  |  |  |  |  |  |  |  |  |  |
|  | ***LEGAL RISKS*** | | | | | | | | | | | | | |
|  |  |  | RiskN | |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Risk management activities (3)** | | | | | | **Evaluation of the risk as the result of activity implementation (4)** | | | | |
| **Activity name** | **purpose** | **type** | **Estimated value of the activity, mln.tenge**  **(specify, if possible)** | **The activity implementation period** | **Person/business unit responsible for implementation of the activity** | **probability** | **Damage size** | | **Period of influence** | **Significance score** |
| **influence** | **Damage amount in thous.tenge** |

**14 15 16 17 18 19 20 21 22 23 24**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***STRATEGIC RISKS (Risks associated with Fund’s strategy )*** | | | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
| ***FINANCIAL RISKS (risks associated with financial activity)*** | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |
| ***OPERATIONAL RISKS*** | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |
| ***LEGAL RISKS*** | | | | | | | | | | |
|  |  |  |  |  |  |  |  |  |  |  |

Column 15: one of the options: А) reduction of damage; B) reduction of probability; C) prevention of risk ;DГ) loss recovery

Column16: one of the options for : А) avoiding risk; B) risk transfer; C) risk reduction; D) risk acceptance

FZ 01 PR 03-03-10

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **The Report on implementation of Action plan for risk management** | | | | | | | | | | | | |
| **№** | **Risk code** | **Risk name** | **Activity name** | **purpose** | | **type** | **Estimated value of the activity, mln.tenge**  **(specify, if possible)** | **The activity implementation period** | **Person/business unit responsible for implementation of the activity** | **The status of activity implementation** | **The score of remaining risk significance** | **Evaluation of activity efficiency (exp.method)** |
| **1** | **2** | **3** | **4** | **5** | | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| **STRATEGIC RISKS (risks associated with the Company’s strategy)** | | | | | | | | | | | | |
|  |  |  |  |  |  | |  |  |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |  |  |
| **FINANCIAL RISKS ( risks associated with financial activity)** | | | | | | | | | | | | |
|  |  |  |  |  |  | |  |  |  |  |  |  |
| **OPERATIONAL RISK** | | | | | | | | | | | | |
|  |  |  |  |  |  | |  |  |  |  |  |  |
| **LEGAL RISK** | | | | | | | | | | | | |
|  |  |  |  |  |  | |  |  |  |  |  |  |

Column 5: one of the options: А) reduction of damage; B) reduction of probability; C) prevention of risk ; D) loss recovery

Column 6: one of the options for : А) avoiding risk; B) risk transfer; C) risk reduction; D) risk acceptance

Column 11: 1 – efficient, 0 - inefficient

Annex 1

**Unified nomenclature on marking key risks**

|  |  |
| --- | --- |
| No.of risk – risk group – short name of the Company | Full name of the risk |
| 1-С-СЭ | The risk of damage to reputation |
| 2-С-ДЗО | Making decisions without taking into account strategic objectives |
| 3-С-СЭ | The risks of Company group’s human resources |
| 4-С-СЭ | Disruption of IPO program |
| 6-С-СЭ | The risk of new investments, including the risks of unsuccessful acquisition of assets  assets |
| 8-С-СЭ | Industrial accidents caused damage to the health and lives of workers in the performance of official duties |
| 9-С-СЭ | Innovations risks |
| 10-С-ДЗО | risks of SA’s implemented investments projects |
| 11-С-Ф | Social risks |
| 12-Ф-Ф | Reduction performance efficiency in connection with high non-commercial load on activity of the Company and its subsidiaries. |
| 13-Ф-ДО | The decrease in market share |
| 14-Ф-ДО | Country risk - the loss of assets (investments) placed (invested) abroad |
| 15-Ф-СЭ, ДО | Lack of liquidity for carrying out operational, investment, financial activities |
| 16-Ф-СЭ | Currency risk |
| 17-Ф-СЭ | Interest rate risk |
| 18-Ф-СЭ | Credit risk |
| 20-Ф-ДЗО | The fall in demand for products |
| 21-Ф-ДЗО, СК | Financing of investment projects |
| 22-Ф-ДЗО | No confirmation of recoverable reserves, low  metal content in the ore |
| 23-Ф-СЭ | Risk of warranty obligations payment |
| 24-Ф-ДЗО | Tariff setting |
| 25-Ф-СЭ | low-quality analysis of the development plans of subsidiaries,  adjusting of development plans and their implementation by the sectoral directorates of the Company |
| 26-О-ДЗО | Fraud / corrupt practices on the part of staff and  third parties |
| 27-О-СЭ, ДЗО | Leakage of confidential information / use of insider information |
| 28-О-СЭ | Procurement process risks |
| 29-О-СЭ | Corporate governance risks |
| 30-О-СЭ | Business processes risks |
| 31-О-СЭ | Information system risks |
| 34-О-СЭ, ДЗО | Safety at work and during the execution of official duties |
| 38-О-СЭ | Accidents and Disasters of power generation sector |
| 39-О-СЭ | Accidents and Disasters of power transmission sector |
| 46-О-ДЗО | Technological risk |
| 47-П-ДЗО | Cancellation, suspension of a license, the prohibition on provision of services in a particular market segment outside of Kazakhstan. |
| 48-П-СЭК, ДЗО | Risk of violation of tax legislation |
| 49-П-СЭ, ДЗО | Legal proceedings (claim-related work) |
| 50-П-СЭ, ДЗО | Risk of violation of the legal regime |
| 51-П-СЭ, ДЗО | The risk of changes in legislation |
| 52-П-СЭ, ДЗО | No registration or late registration of subsoil agreements |
| 53-П-СЭ, ДЗО | Seizure of property (assets) |

# Annex 2

**Questionnaire for risk identification**

|  |
| --- |
| Questionnaire |
| Date of completion: |
| Full name of an employee: |
| Business unit: |
| **1 – Make a SWOT-analysis on the activity of your business unit specifying:**  **a) Strong internal factors (Strengths);**  **b) External factors that provide opportunities (Opportunities);**  **c) Weak internal factors (Weaknesses);**  **d) External factors that constitute threat (Threats)** |

|  |  |
| --- | --- |
| **strengths:** | **weaknesses:** |
| **opportunities:** | **threats:** |

|  |
| --- |
| **2 - On the basis of conducted SWOT-analysis, identify key risks that have a negative impact on the achievement of strategic objectives by your business unit.** |

|  |  |
| --- | --- |
| Risk No.1 |  |
|  |  |
| Risk No.2 |  |
|  |  |
| Risk No.3 |  |

|  |
| --- |
| **3 - Identify factors (causes) of risk for each risk identified in paragraph 2.** |

|  |  |  |
| --- | --- | --- |
| Risk No.1 | 1 |  |
|  | 2 |  |
|  | 3 |  |
| Risk No.2 | 1 |  |
|  | 2 |  |
|  | 3 |  |
|  |  |  |
| Risk No.3 | 1 |  |
|  | 2 |  |
|  | 3 |  |

|  |
| --- |
| **4 - Determine possible consequences of each risk identified in paragraph 2.** |

|  |  |  |
| --- | --- | --- |
| Risk No.1 | 1 |  |
|  | 2 |  |
|  | 3 |  |
|  |  |  |
| Risk No.2 | 1 |  |
|  | 2 |  |
|  | 3 |  |
|  |  |  |
| Risk No.3 | 1 |  |
|  | 2 |  |
|  | 3 |  |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |  |  |

**Questionnaire on risks**

(annual interviewing)

1. What risks have occurred during the past calendar year in your business unit that led to losses (fines, lost profit, additional costs, etc.)?

2. What risks have occurred during the past calendar year in your business unit that entailed adverse effects (influence on the Company's reputation, expired control orders, etc.)?

3. What risks may affect the achievement of goals and tasks set to your business unit?

4. What risks are more likely to occur that will affect the achievement of goals and tasks set to your business unit?

5. What risks are inherent in the activities of your unit which may affect the achievement of strategic goals of the Company?

6. What negative effects may arise upon occurrence of risks (events) in your business unit, and what is possible amount of damage?

7. What measures will be taken to mitigate risk, i.e. to reduce the likelihood of occurrence of negative events or damage caused by risk occurrence or adverse events?

Annex 3

**Questionnaire on risks**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Risk name | Company’s exposure to risk | If YES, please evaluate the probability of influence, the period of influence of a risk  by checking the appropriate box | | |
| Frequency or probability of a risk | Risk influence | Risk impact period |
| 1 |  | yes  no | Once in 7 and more years (or the probability of occurrence is up to 5%) | Absence of any consequences in the event of risk occurrence | Time for correction is available. |
| Once in 5 years (or the probability of occurrence 25%) | Consequences of risk occurrence are not significant | Influence of risk shows up with time lag |
| Once in 3 years (or the probability of occurrence 40%) | Consequences of risk occurrence are not significant and can be fully improved | Risk appears immediately |
| Once in year (or the probability of occurrence 80%) | Consequences of risk occurrence are very significant but may be improved to a certain extent |  |
| Once in a half year and often (or the probability of occurrence is over 95%) | In case of risk occurrence, the company almost cannot recover from consequences of this risk |  |
| 2 |  | yes  no | Once in7 or more years (or the probability of occurrence is up to 5%) | Absence of any consequences in the event of risk occurrence | Time for improvement is available |
| Once in 5 years (or the probability of occurrence 25%) | Consequences of risk occurrence are not significant | Influence of risk shows up with time lag |
| Once in 3 years (or the probability of occurrence 40%) | Consequences of risk occurrence are not significant and can be fully improved | Risk appears immediately |
| Once in year (or the probability of occurrence 80%) | Consequences of risk occurrence are very significant but may be improved to a certain extent |  |
| Once in a half year and often (or the probability of occurrence is over 95%) | In case of risk occurrence, the company almost cannot recover from consequences of this risk |  |

**Annex 4**

**Classification of events that caused loss**

|  |  |  |  |
| --- | --- | --- | --- |
| **Category of event type (1st level)** | **determination** | **Category (2nd level)** | **Examples of activity type** |
| Internal fraud | losses due to actions  with intention to commit a fraud, to assign property or circumvent regulations, the law or internal regulations of the Company, with the participation of at least one internal party | Unauthorized activity | Transactions not mentioned in the report  (intentionally)  Unauthorized types of operations (entailing financial losses) Incorrect assessment of the position (intentionally) |
| Fraud and theft | Fraud  Theft, extortion, robbery  Assigning assets  The deliberate destruction of assets  Forgery  smuggling  Assigning foreign accounts / use of someone else’s documents, etc.  Deliberate failure to comply with tax laws or tax evasion  bribes  Insider trading (not by the Company’s means) |
| External fraud | losses due intent to commit fraud, steal property or violate the law involving a third party | Fraud and theft | Theft, robbery  forgery  writing out bad checks |
| Systems safety | Hacking, data theft entailed a financial loss |
| Human Resources  policy and occupational safety | losses due to violation of labor legislation, occupational safety and health, or in connection with the payment on claims for personal  damages or claims in connection with  discrimination | Relationship with employees | Matters on wages, remuneration and  Severance payments  Organization of labor activity |
| Safe environment | General obligations on accidents |
| discrimination | All types of discrimination |
| Personnel qualification | Insufficient qualification of personnel |
| Customers, products and business practice | losses due to  unintentional negligence in the performance of professional obligations in relation to specific customers (including trust and qualification requirements) or due to the nature or design of the product | Eligibility,  disclosure, fiduciary relationships | breach of fiduciary relations /breach of instructions, problems of information disclosure (Know Your Customer)  Violation of requirements on disclosure of information to retail customers  violations related to disclosure of personal confidential information  aggressive sale  artificial overcharging (fees)  abuse of confidential information  lender obligations |
| Incorrect  business or market practices | Anti-monopoly legislation  Improper trading practices / market operations |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | market manipulation  Insider trading activities activity without a license Money laundering |
| Product imperfections | Product Defects  Design errors |
| Choice, sponsorship  and Risks | Failure to comply with requirements of the customer study  Exceeding the risk limit per customer |
| Consulting services | discrepancies in the assessments of consulting services results |
| Causing damage to physical assets | Losses as a result of damage  or damage to physical assets from natural disaster or other events | Disasters &  other events | The damage caused by natural disasters,  human losses from external sources (terrorism, vandalism) |
| Violations in  conducting business and system failures | losses due to violations in conducting business  and system failures | systems | software  Hardware  Telecommunications  Disruptions in energy supply and provision of public services |
| Performance,  delivery and process management | Losses as a result of failure  in processing operations or failures during or as a result of relationships with trade counterparties and vendors | Performance and  Operations support | Incorrect communication ,error  when entering, loading or maintenance of data  Violation of terms or obligations  Malfunction of systems or models  Accounting mistakes / errors in counterparty attribution  Other errors when performing tasks  Disruption of Delivery  Failures in pledge management  maintaining of reference data |
| Monitoring and reporting | Failure to comply with mandatory reporting  inaccurate external reporting that entailed losses |
| Attraction of customers and documentation management | The lack of permits / exemption of  Liability from customers missing or incomplete legal documentation |
| Customer accounts management | Unauthorized access to accounts  Incorrect client records that entailed losses  The damage or loss of customers as a result of negligence |
| Trade counterparties | Incorrect operations of counterparties  Conflicts with contractors |
| Suppliers and contractors | Outsourcing  Conflicts with suppliers |