Appendix to Resolution
of Board of Directors
of Almaty Electric Stations JSC
dated “_29__”____05_______2025
(Minutes №04/25___)

Rules for identifying and assessing risks of Almaty Electric Stations JSC

Document owner	Corporate Development and Risks Department, CDRD
Edition	2
Year	2025

Almaty

REFERENCE COPY

Content

1. Appointment and scope of application

These Risk Identification and Assessment Rules (hereinafter referred to as the Rules) are developed in accordance with the Risk Management Policy of AlES JSC (hereinafter referred to as the Policy), Risk Identification and Assessment Rules of Samruk-Energy JSC and other internal regulations governing the activities of AlES JSC (hereinafter referred to as the Company).

The Rules determine the order, procedures, methodology of risk identification and assessment, as well as control over current risks and monitoring of efficiency of risk management methods. More detailed approaches to risk assessment can be reflected in the documents regulating the process of management of individual risks of the Company.

Identification of risks and availability of a real objective view of available risks is one of the bases of effective risk management, assisting in achievement of the Company's goals.

Risk identification provides a tool for registering and declaring possible negative events that may adversely affect the achievement of goals and objectives set for the Company and each of its employees, as well as determining the direction and the need to improve the risk management process.

These Rules apply to all types of the Company's activities. The Rules are mandatory for familiarization and application by all structural subdivisions and all employees of the Company. When performing their functional duties and realizing their tasks, each employee of the Company shall be guided by the provisions set out in the Rules.

Compliance with the Rules is mandatory for all employees of the Company.

2. Responsibility

2.1 The structural division of the Company in charge of risk management - Corporate Development and Risks Department (hereinafter - CDRD) is responsible for organization of risk assessment.

The CDRD coordinates the work with all divisions of the Company. Questionnaires conducted by the CDRD, as well as enquiries on key risks are mandatory for all subdivisions and personnel of the Company.

CDRD provides support to structural divisions of the Company in the process of identification and assessment of risks, and also carries out consolidation of risks of the Company.

Responsibility for improvement of methods of identification and assessment of risks in the Company shall be borne by CDRD.

Responsibility for the management of these Rules shall be borne by CDRD.

2.2 Legal Affairs Managing Director supervising the activities of the Risk Management and Risk Control Department submits the issues of identification of critical risks of the Company, as well as proposals for their management to the Management Board of the Company, which in turn submits the issues of critical risks to the Board of Directors of the Company.

2.3 Responsibility for provision of timely, reliable, full and adequate information used for formation of the register of risks, the plan of measures on minimization of key risks of the Company is borne by owners of risks.

Risk owners are responsible for timely informing and identification of realized risks.

3. Terms and abbreviations

Term | abbreviation	Definition
Risk occurrence	risk incidence rate;
Risk owner/Risk holder	A person (employee/structural unit/collegial body) responsible for all aspects of managing a certain risk, in particular, reducing the probability

	of risk realization and / or reducing the possible impact of the consequences of risk realization on the Company;
Impact	value of potential loss that may arise in case of risk realization;
Time of impact	duration of risk impact;
Corporate Development and Risk Management	structural division of the Company responsible for risk management;
Risk map	Graphical and textual description of a limited number of risks of the Company located in a rectangular table, one axis of which indicates the strength of impact or significance of the risk, and the other axis indicates the probability or frequency of its occurrence. On the map the probability or frequency is displayed on the horizontal axis, and the strength of impact or significance - on the vertical axis. In this case, the probability of occurrence of a risk increases from left to right as you move up the horizontal axis, and the impact of the risk increases from bottom to top on the vertical axis;
Residual risk	the risk remaining after the risk owner has taken action to change the likelihood or degree of impact of the risk;
Risk assessment period	date, at the end of the reporting period;
Inherent risk	is the amount of risk in the absence of action by risk owners to change the likelihood or degree of impact of the risk on the achievement of the organization's objectives;
Amount of loss	the amount of projected damage due to the realization of the risk;
Risk register	a list of the risks faced by the Company in its activities, which also includes the risk of the Company's exposure to the risk. For each risk, risk owners are identified, i.e. the departments that deal with this risk by virtue of their functional responsibilities
Society	Almaty Energy Stations Joint Stock Company;
SDC	Structural subdivision of the Company
Near Miss	A non-consequential event or any event that could reasonably have resulted, but did not as a result of a combination of circumstances, in damage to people, assets, the environment, the Company's reputation or a combination of these consequences.

4. Rules for risk identification and assessment

The employee of structural division of the Company responsible for the organization of activity on risk management reflects his vision of available risks in questionnaires, according to the Appendix 7 of the present Rules on an annual basis, or during other actions carried out by CDRD aimed at identification and an estimation of risks of the Company.

Based on the identified events the register of risks which represents the systematized list of the risks faced by the Company is prepared.

4.1 Identification of risks

Risk identification is important as a method of optimization of the Company's expenses, since early identification of risks, determination of adequate measures for their minimization and elimination of consequences allows planning sources and volumes of financing of such measures, which ultimately affects the efficiency of the Company's activity. A combination of various techniques and tools is used to identify risks. Events are identified both in terms of past experience and future possible events. The main techniques are described below.

Risks can be identified using two approaches:

1) initial identification and inventory of risks - initial compilation of the Company's Risk Register when implementing the risk management system and its regular review.

In the course of the initial identification of risks the Company's Risk Register is compiled in order to carry out subsequent assessment and determine approaches to the management of these risks. The process of risk inventory implies regular (at least once a year) revision of previously identified risks, i.e. determination of relevance and materiality level of the risks in the Company's risk register. As a result of inventory some of previously identified risks can be recognized irrelevant;

2) detection of potential risk - revealing of potential risk in the course of current activity.

New risks may be identified not only in the course of execution of regular procedures within the risk management system, but also in the course of current activities of the Company's employees. If information on a potential risk not previously included in the register is discovered, an employee of a structural subdivision should send a corresponding memo to the Risk Management and Risk Control Department, which sets out the information and lists the expected consequences of the risk event. CDRD analyses and evaluates the information received and, if necessary, includes the new risk in the risk register of the Company.

4.1.1 Identification of risks on the basis of set goals and objectives. Based on the set goals or balanced scorecard, potential events that may affect their achievement are identified. Events are identified by owners of risks and pass coordination with UKR&R, and on this basis the register of risks is made (or corrected or supplemented).

4.1.2 Industry and international comparisons. The register of risks is made on the basis of the list of potential events characteristic for the organizations similar to the Company and (or) the organizations on branch specialization or functional activity.

4.1.3 Seminars and discussions. The risk register is compiled on the basis of an organized discussion (brainstorming, round table, etc.) of potential events that may affect the organization and the achievement of its goals with the Company's employees. Such discussions may be held within each structural unit to identify events (risks) affecting the activities of each such unit and the Company as a whole, then the results are integrated into the risk register (or the existing risk register is supplemented/corrected).

4.1.4 Interviewing. Risk Management Department conducts targeted interviewing of key employees (experts) of the Company for open discussion of existing and potential risks and ways to manage them. Usually such interviews are conducted with STR managers.

4.1.5 Monitoring of publications and speeches. In order to identify risks, publications about the Company, speeches of the heads of relevant ministries and agencies, opinions of industry experts are monitored on a regular basis, draft regulatory documents, industry development concepts, analysts' forecasts, materials of relevant conferences, etc. are analyzed.

4.1.6 Analysis of reports on the results of audits and other inspections. This method is an inspection of individual areas of the Company's activities and may be combined with individual expert methods (questionnaires, interviews). Compliance between the available documentation and actual practice of application of regulations is checked, the regulatory framework and instructions are analyzed, and as a result a conclusion is prepared on the basis of which risk identification is carried out.

4.1.7 Near Miss analysis consists in registration of all facts of violation of regulations (operational, production, etc.), and forecasting on their basis of probability of occurrence of risk events. Thus, due to uncertain factors, violation of regulations may not immediately lead to the realization of a risk event, but the probability of occurrence of this risk event is higher and more unexpected, the more facts of non-realization of the risk event. Near Miss is an incident that, under certain circumstances, could have resulted in injury, fire, spill, accident, etc., but did not. Statistics show that for every 600 Near Miss there is a high probability of a significant incident - the realization of a risk event.

4.1.8 Database of incurred losses. The Company continuously monitors incurred losses, information on which also allows identifying events that have a negative effect on the Company's operations. In addition, the database of incurred losses is a good basis for quantitative risk assessment. The database is formed on the basis of reports of the Company's structural divisions and may also include data from external sources. This method includes:

1) analysis of data on violations - analysis of reported violations, extraordinary situations, failures in the Company's processes and other facts of deviation of indicators of current activities from the planned ones;

2) analysis of reporting - analysis of the Company's reporting and other documentation, including management, accounting, tax reporting, the Company's performance indicators, plans, contract registers, etc.;

3) analysis of other companies' experience - comparative analysis of the Company's processes and indicators with other large companies. Periodicals and reports of specialized agencies may be used for analysis.

Identified events and risks are systematized in the form of the register of risks according to the Appendix 1 of these Rules. The form and level of detail of the register of risks can change with development of risk management system. Grouping of risks can be realized, proceeding from the nature of risks, their interrelation, and also on the basis of other factors (for example, use of concrete methods of risk management).

4.1.9 The register of risks of the Company represents the list of risks which the Company faces in its activity, distributed on four main categories of risks which also includes various scenarios of possible realization of risk. Risk owners are defined for each risk.

The risk register consists of 4 parts:

1) risk passport, which specifies the KPI, its threshold value, the name of the risk that may prevent the achievement of the KPI, the cause of the risk, a description of the possible consequences from the realization of the risk, the key risk indicator and the risk owner;

2) assessment of inherent risk - in this part the risk is assessed by probability, impact and time of risk impact. Calculation of the significance score shall be performed in accordance with these Rules;

3) risk management measures - this part specifies risk management measures, indicating whether they are current or planned;

4) risk assessment as a result of the implementation of measures - the risk assessment as a result of the implementation of measures shall be performed. This part of the register allows evaluating the effectiveness of risk management measures.

Systematization of identified risks allows:

1) achieve consistency in the classification and quantification of risks, which allows to improve the comparison of the Company's risk profile (by business processes, structural divisions, projects, etc.);

2) provide a platform for building more sophisticated tools and technologies for quantitative risk assessment;

3) to provide an opportunity for coordinated management and control of risks of the Company.

For the purpose of standardization of the register of risks and consolidation of risks in the risk map of AlES JSC, the Company uses the unified nomenclature given in Annex 2 of the present Rules on designation of the main risks.

For definition of risk nomenclature the following format is used: 'Risk number'-'Risk category'-'Abbreviated name of the company'. For example, for currency risk of the Company, following the designated format will be: '5-F-AlES', which means: risk number '5', with the category "financial", the owner of the risk is Almaty Electric Stations JSC.

The Company uses the nomenclature of risks, given in Annex 2 of these Rules for designation of risks, for the purpose of consolidation of critical risks of the Company into the consolidated risk register of

Samruk-Energy JSC.

If there is no risk specific to the Company in the risk nomenclature, then the Company shall designate this risk, adhering to the above-mentioned format using continuing numbering (numerical numbers in the numbers of risks designated in the nomenclature cannot be used to designate other risks).

The register of risks is revised, specified or supplemented on an annual basis or more often as information on risks provided by structural divisions of the Company at identification of new or change of a status of existing risks to the Chief risk specialist. At inclusion in the register of risks of a new risk or change of a status of existing risk with potential influence above level of restraining ability and high probability of its realization, CDRD brings the information on such risk with offers on its minimization to the notice of the Board of Directors of the Company.

Responsible for carrying out measures on identification of risks and formation of the register of risks is CDRD. The register of risks is subject to coordination with owners (owners) of risks.

The Risk Management and Control Department are the structural subdivisions of the Company responsible for providing information on risks, including critical risks.

The process of identification of operational risks is carried out as part of the process of identification and assessment of risks on an ongoing basis in accordance with these Rules and other internal regulatory documents of the Company.

Depending on circumstances (reasons) of operational risks occurrence, events or cases of operational risks manifestation are classified by risk factors as follows:

1) external frauds - robberies, forgery and falsification of documents, theft of documents/information, hacking/breaking into information systems and other cases that occurred through the fault of third parties;

2) internal frauds - cases of losses caused by intentional actions of the Company's personnel, including abuse of office, intentional concealment of transactions, information leakage, embezzlement, fraud, extortion, embezzlement of material assets, misappropriation or intentional damage to the Company's property;

3) Labor relations - cases of labor disputes with employees, violation of labor law provisions, including health and safety requirements, high staff turnover, disclosure of confidential information by employees, insufficient qualification of personnel;

4) clients and business practices - cases of violations of legislation in the course of the core business; non-fulfillment or improper fulfillment of obligations arising from contracts related to the core business to clients, counterparties and other third parties; violations of business practices;

5) failures in information and technical systems - failure of equipment and systems and, as a result, loss of information data, late submission of reports to supervisory authorities, etc..;

6) process management - inadequate organization of internal processes and procedures, violations of established limits, lack of protection system and information access procedure, improper organization of information flows within the Company, errors in entering and processing data on operations and transactions, etc..;

7) damage to tangible assets - loss or damage to fixed assets and other tangible assets as a result of objective situations beyond the Company's control (man-made);

8) industrial accidents - events that caused damage to the health and life of employees in the process of performing their functional duties.

Classification of indicators is given in Appendix 3 to the Rules, which can be changed and supplemented as various cases of operational risk arise.

4.2 Risk Assessment

Risk assessment allows the Company to analyze the impact of a potential risk on the achievement of its objectives. Risks are assessed in terms of the likelihood or frequency of their occurrence and impact, using a combination of qualitative and quantitative methods where possible. The positive or negative impact of potential risks shall be assessed individually or in interrelationship across the Company. Risks are assessed in terms of their full impact (gross risks).

The risk assessment process is carried out in order to highlight the most significant risks that may negatively affect the Company's activities and the achievement of its strategic goals and objectives. These risks are submitted for consideration of the Board of Directors of the Company and decisions on their management and control are made.

Initially risk assessment is carried out on a qualitative basis, then for the most significant risks it is necessary to strive for quantitative assessment of risks with application of the approaches to assessment described below depending on a concrete situation. So, for example, at an estimation of technological risks it is necessary to make calculation of risks on the basis of cost of the property, on the basis of the lost income, etc. Risks that cannot be quantified or there is no reliable statistical information for modeling or building such models is not cost-effective, are assessed only on a qualitative basis.

Quantitative assessment provides more accurate analyses and is particularly useful in developing risk financing methods.

At the stage of preparation of qualitative risk assessment, the main parameters of such assessment are established. Risk assessment is carried out on three indicators - frequency or probability of risk; time of influence and size of risk. To ensure comparability of risks among themselves and to facilitate qualitative assessment, a point scale is introduced.

Frequency or probability of risk

Score	Definition	Frequency or probability
1	Very rarely	Every 7 or more years (or up to 5% probability of occurrence)
2	Rarely	Every 5 years (or 25% probability of occurrence)
3	Occasionally	Every 3 years (or 40% probability of occurrence)
4	Often	Every year (or 80% probability of occurrence)
5	Very often	Every six months or more (or over 95% probability of occurrence)

Time of risk impact

Score	Time impact
1	Time to correct
2	The impact of the risk manifests itself with a time lag
3	The risk manifests itself with an immediate effect

Risk impact assessment is carried out in monetary terms on the basis of the Company's risk appetite defined in the Policy. For reporting purposes, the Company uses the assessment of the impact of critical risks according to the following table.

Risk exposure (financial indicators)

Score	Definition	Potential loss from risk occurrence
1	Minor	Below 25% of risk appetite level
2	Notable	25-50% of risk appetite level
3	Major	50-75% of risk appetite level
4	Critical	From 75% of risk appetite level up to risk appetite value
5	Catastrophic	Above risk appetite level

When submitting quarterly information to Samruk-Energy JSC, the Company provides a risk map with indication of critical risks.

After implementation of the risk-oriented financial model in the Company, the transition to quantitative assessment of risks will be made on the basis of CashFlow at Risk indicator. Potential damage from realization of risk will be calculated on the basis of historical data from the database of realized risks, using the method of Monte Carlo simulation modeling.

For risks which influence is difficult to estimate in financial indicators (for example, risks of the personnel, reputation, etc.) characteristics showing the size of risk in comparable points are entered. Non-financial indicators of the significance of risks can be determined on the basis of balanced indicators taking into account the materiality of deviation from the objectives.

Non-financial indicators of risk impact.

Score	Degree of influence	Potential loss from the occurrence of the risk
1	Insignificant	No consequences in case of risk realization
2	Low	The consequences of risk realization are not significant
3	Medium	The consequences of risk realization are not significant and can be fully remedied
4	Significant	The consequences of risk realization are very significant but can be remedied to a certain extent
5	Catastrophic	In case of risk realization, it is practically impossible for the company to recover from the consequences associated with this risk

The register of risks and a point scale of an assessment of risks on frequency (probability), time of influence and size (influence) of risk is brought to key employees (experts) of the Company for carrying out qualitative assessment of risks.

Qualitative assessment of risks is carried out either by target interviewing of key employees or by questionnaire, when experts are offered to choose risks which they consider the most significant for the organization, to estimate them on the offered point scale, and also to give offers (recommendations) on their management. A combination of both methods may be used: a broad questionnaire survey of the Company's employees based on the electronic questionnaire system and interviewing of heads of structural divisions, Managing Directors of the Company, except for members of the Management Board of the Company.

When carrying out expert risk assessment, experts should apply net assessment only on condition that current measures are assessed by experts as effective. At the same time, the assessment of the effectiveness of measures should be confirmed. Otherwise, risk assessment is carried out on an inherent basis.

The obtained results are processed: for each risk, risk scores are calculated on the basis of the aggregate assessment of experts, risks are assigned a significance coefficient and a risk map is built on this basis.

The calculation of the Risk Significance Score is carried out as follows:

Significance Score = (frequency + realization time)* impact,

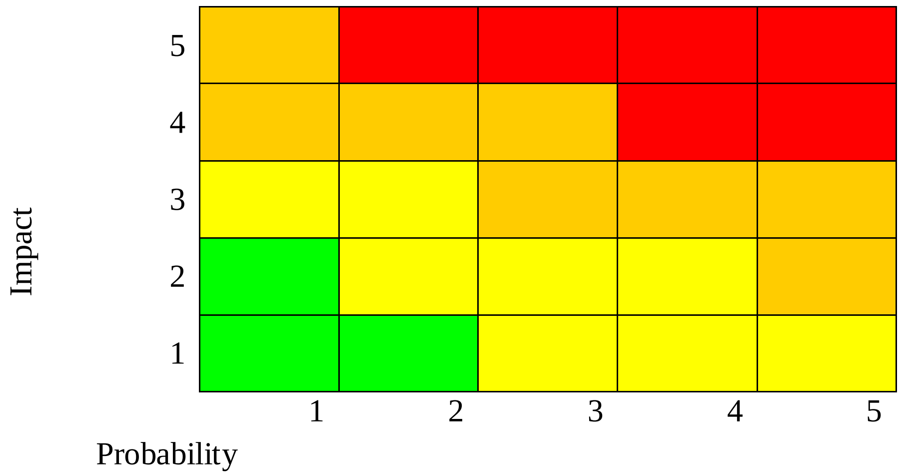
To assess operational risk, on the basis of the Risk Significance Score, the value of operational risk rating (RR) of each type of risk is determined according to the table below:

Risk significance score	Risk rating value, RR	Overall risk significance	Definition
28,1 up to 40	1,00	Extremely	Risk response measures shall be identified or, if any, improved, prepared for implementation before the start of project/task implementation or immediately after risk identification at the stage of project/task implementation.
15,01 up to 28	0,9	High	Risk response measures shall be identified or, if any, improved and implemented within 1 month in the course of project/task implementation.

8,01 up to 15	0,8	High	Risk response measures shall be identified or, if any, improved within a period of up to 3 months and implemented in the course of project/task implementation.
1,01 up to 8	0,6	Medium	Risks of this category shall be controlled, but preparation of response measures is not required.
0 up to 1	0,5	Low	

The risk map allows to assess the relative importance of each risk (compared to other risks), as well as to highlight the risks that are critical and require the development of measures to manage them. The construction of the risk map allows:

1) determine the potential of risk retention within the framework that can be applied to all operations of the Company;
2) to develop a list of critical risks of the Company and ensure the availability of appropriate processes for their management;
3) Priorities risks and develop the allocation of financial resources.
4) The risk map is divided into several areas highlighted in different colors.
5) Red zone - risks that are critical for the Company either due to a high probability of occurrence or due to a serious potential for damage that may affect the financial stability of the Company;
6) orange zone - risks that have a high probability of occurrence or a major potential impact on the financial stability of the Company;
7) yellow zone - risks that have medium probability of occurrence or medium potential impact on the Company's financial stability;
8) green zone - risks that have a low probability of occurrence and (or) have no significant impact on the Company's financial stability.



Identification numbers of risks (according to the register of risks) according to indicators of frequency (probability) of occurrence and size (influence) of risk are put on the map.

The risk map is a graphical representation of the Company's exposure to critical risks and is a mandatory appendix to the risk management report for the Board of Directors.

Priority of risks is established according to position of each risk on the risk map:

1st group - catastrophic and critical risks - red zone of the risk map - risks having the highest priority. Such risks which make 75 % and above level of risk-appetite, and also exceed risk-appetite;

2nd group - large risks - orange area of a map of risks - the second on priority risks, damage from realization of which remains within 50-75 % level of risk-appetite;

3rd group - average risks - yellow area of a map of risks - the third on priority risks, damage from realization of which remains within 25-50 % level of risk-appetite;

4th group - low risks - green area of a map of risks - risks within up to 25 % level of risk-appetite;

Within each of the groups, the prioritization of risks is established on the basis of the risk significance score.

Each of the risks included in prioritization groups 1, 2 and 3 are assessed based on the following factors:

- analysis of reasons of occurrence of risks (scenarios of losses);
- analysis of potential influence of risk on financial indicators of the Company - gross (without taking into account methods of risk management) and net (residual risk after application of methods of risk management);
- analysis of correlation of risks with other risks (repayment of negative effect from occurrence of risk in one division by positive in other division - principle of compensation, or strengthening of negative effect in connection with occurrence of other risks - principle of dominoes).
- The size of the impact of critical risk should be quantified. In case of impossibility or impracticality of quantitative assessment, it is necessary to make a detailed risk assessment using a combination of qualitative assessment methods to achieve the most reasonable assessment. In quantitative assessment, the risk is always assessed first on a gross basis, then on a net basis, taking into account the risk management measures taken. On the map, a change in risk can be reflected by moving the corresponding identification number.

The risk is quantified on the basis of the maximum possible damage from the occurrence of each specific risk. Various methods and models can be used for quantification.

Risk assessment methods include:

- quantifying risk based on the value of property that could be damaged by the occurrence of the risk. This model constructs scenarios of material damage when the risk occurs, and calculates the replacement value of property that could be damaged and subsequently repaired or replaced. Usually used for quantitative assessment of operational risks (material damage to property as a result of man-made disasters, fire, etc.);
- quantitative assessment based on the calculation of lost income. The duration of possible production downtime as a result of the risk occurrence is estimated and the income (or fixed costs) per day is calculated. Multiplication of these indicators results in a quantitative assessment of risk. Such an assessment is usually used to assess the risks of production interruption or supply disruption;
- quantitative risk assessment based on comparative analysis. Estimation of the maximum damage from some types of risks, for example, risks of liability for damage or environmental pollution, cannot be calculated by any formulae, and therefore precedent statistics (industry and territorial) are used to quantify such risks. To assess such risks, the scenarios of their occurrence and the parties that may be involved (suffer damage), as well as the overall impact of such risk are usually assessed, and the maximum possible damage is determined on the basis of existing information (statistics) on the cost of damage in the realization of such scenarios. Precedent statistics is also used when assessing the impact of any risks on the market value of shares and other securities of the company;
- quantitative risk assessment based on statistical models. Such assessment is used for risks that have a specific monetary expression and dependence on certain external factors (e.g., fluctuations in oil prices, exchange rate fluctuations, inflation expectations, etc.) and is based on the construction of statistical dependencies (e.g., using regression analysis methods). In this case, it is possible to clearly determine under what conditions the risk may be material for the corporation.

The statistical approach is based on historical data of realized risk events. At this approach quantitative assessment of risks is made on the basis of the accumulated internal or external statistics. The main methods of risk assessment within the framework of this approach:

- value-at-risk (Value-at-risk - VaR) - the maximum decrease in the value of a financial investment on a certain planning horizon (for example, a month), which will not be exceeded with a high (predetermined) probability (usually 95% - VaR95% or 99% - VaR99%). The value of VaR has a monetary expression;
- cash-flow-at-risk (CFaR) is the maximum decrease in the value of cash receipts (or maximum increase in expenses), caused by the impact of one or more risk factors, which will not be exceeded with a high (predetermined) probability (usually 95% or 99%) at a certain planning horizon. The method reflects the specificity of risks of non-financial companies.

Since most assets of non-financial companies are illiquid, the main risk for them is a decrease in operating cash flows. Therefore, the key value metric of risk is cash flows at risk. In this regard, it is necessary to build a model describing the impact of one or a group of factors on the amount of cash receipts (expenses) of the Company. Risk factors can be both market values (prices, exchange rates, interest rates) and random events (credit, operational, regulatory, etc.). Possible changes in risk factors and probabilities of such changes are estimated based on historical data or expert judgments. Based on the constructed model, possible changes in factors are transformed into possible changes in cash flows, and a probability distribution of changes in cash flows is constructed. The CFaR method can be applied to assess the risk of cash flow changes for a separate type of the Company's activity or for the Company as a whole. The CFaR value shows the largest changes in cash flows on a certain planning horizon, while maintaining on the whole horizon all probability distributions of risk factors and models of influence of these factors on the formation of cash flows;

- Earnings-at-risk (EaR) - this method of quantitative calculation of risks is an analogue of the CFaR, but takes into account accounting aspects of the Company's income recognition. One of the main differences between SFaR and EaR is the cost metric of risk. Unlike CFaR, where the value metric of risk is cash flows, in calculating EaR the value metric of risk is the future profit of the Company;
- quantitative assessment of risks on the basis of stochastic (probabilistic, Monte Carlo method) models. Such an assessment is used when assessing risks that can be expressed in monetary form, but the correlation dependence on external factors is rather difficult to establish, since the risk has a clearly expressed probabilistic nature. Such risks, for example, may include the risk of natural disasters.

In this approach, various scenarios of risk events are modeled and the impact of the consequences of risk events on planned cash flows and financial and economic results of the Company's activities is analyzed.

The main method of risk assessment within the framework of stochastic (probabilistic) models is Stress testing. The method helps to determine losses that the Company may incur in case of realization of unexpected unfavorable events. Stress testing does not give a single quantitative value of risk as an output. This method makes it possible to assess the consequences of various unfavorable scenarios and the Company's 'margin of safety' in relation to risk factors. Since the scenarios considered within this method are realizations of rare events, no probabilities are attributed to them during stress testing. Stress testing consists of two stages:

- building a model of the impact of risk factors on the company's cash flows (similar to the CFaR method);
- developing scenarios of risk factor realizations.

In order to build the model it is necessary to identify the segment of cash flows of the company, which will participate in stress testing (the most effective is the analysis of all cash flows, but it is also possible to consider cash flows on individual financial instruments, or on individual activities). Then it is necessary to identify risk factors affecting the value of selected cash flows. The relationships between the effects of risk factors and cash flows from the necessary model. It may be very simple for a single financial instrument (e.g., a floating-rate loan - the value of each payment depends on the rate change in a strictly defined and obvious way), but for the cash flow of the company as a whole, the dependencies can be complex.

After creating the model, the following should be done:

- enter several stress scenarios into the model;
- assess changes in cash flows when the risk factors (parameters) included in the scenarios change;
- highlight those scenarios for which the change in flows goes beyond the specified materiality criterion;
- analyze possible ways to reduce the exposure to the risks involved.
- Two types of scenarios are used in stress testing:
- single-factor scenarios - the impact of only one risk factor is considered, for example, a strong change in the price of a certain type of service, exchange rate, default of a certain counterparty, etc. This method is interesting only for assessing the company's 'margin of safety' in relation to one of such events. The larger the value of a change in a risk factor that does not lead to a significant change in cash flows, the less the company is exposed to this type of risk;
- multifactor scenarios - simultaneous change of several factors, which is more likely in practice.

Stress testing can be conducted under:

- historical scenarios - based on replicating events that took place in the past. For example, the same changes in factors (exchange rates, interest rates, etc.) and the same events (defaults) that occurred during any selected financial crisis are considered;
- hypothetical scenarios - allow to go beyond historical events. These scenarios require the work of experts. Special consideration should be given to worst-case scenarios (all factors considered take the worst value ever observed), and scenarios with the worst correlations;
- Monte Carlo simulations. This method involves a large number of trials - one-off simulations of market developments. To generate random numbers, the expected (average) value and standard deviation (σ) of historical values of various parameters are taken.
- As a result of these tests, a distribution of possible financial results will be obtained, on the basis of which a VaR or CFaR-estimate can be obtained by cutting off the worst ones according to the chosen confidence probability. The VaR or CFaR value is estimated in the following sequence:
  - the expected (average) value and standard deviation (σ) of each parameter are estimated;
  - random values of each parameter are generated within a given average value and standard deviation, with different results each time;
  - the amount of loss (price change) corresponding to a given probability is determined.

The application of these methods of risk assessment and forecasting will be possible with the introduction of a financial and economic model in the Company.

Often for reliable quantitative assessment of risks it is necessary to apply a combination of some or all of the above methods, or specially developed methods. For many risks mathematical models can be constructed which allow to receive estimations of their quantitative influence depending on various factors, and allow to 'play scenarios' of occurrence of risks.

Quantitative assessment of risks is necessary to understand the significance of each specific risk, to assess the cost-effectiveness of managing such risks, as well as to establish the parameters (terms) of contracts when transferring risk to third parties. The degree of accuracy of quantitative assessment is determined by the needs of the Company, but in any case, such assessment will only provide guidelines for the Company, i.e. the so-called 'corridor'. The Company's task when carrying out quantitative risk assessment is to ensure that this 'corridor' is not only wide enough for all possible consequences to fit within its limits, but also narrow enough not to pay excessive amounts for risk transfer.

Quantitative risk assessment allows stress analysis of the company's financial indicators for risks - in terms of profitability, long-term financial stability (capitalization) and liquidity. If the potential impact of a risk exceeds the limits of the Company's risk appetite, the risk is classified as critical risk.

Assessment of operational risk involves assessment of the probability of occurrence of events causing operational risks and assessment of the risk impact on the Company's activities. Operational risk assessment is carried out from two perspectives - qualitative and quantitative:

- quantitative risk assessment is of a probabilistic (forecast) nature, with the calculation relying on statistical methods;
- qualitative method is used for objects and categories of operational risk, the level of which cannot be unambiguously expressed through some number characterizing the possible level of losses..

The following methods may be used to determine the level of operational risk:

- statistical analysis of sources of operational risk and actual losses;
- point-weighted method.

The method based on the application of statistical analysis of sources of operational risks allows making a forecast of potential operational losses based on the size of operational losses that occurred in the Company in the past. When applying this method, information accumulated in the analytical database on events related to operational risks is used as input data.

In order to build mathematical models for quantitative assessment of operational risks, a statistical database of events related to operational risks for at least 5 years of the Company's activity is required. Until then, the CDRD performs quantitative assessment of operational risks on the basis of calculation of probability of losses from operational risks, based on the number of events related to operational risks and the number of cases of manifestation of operational risks.

Structural divisions of the Company, carry out monitoring of operational risks annually, within the framework of process of identification of risks.

Additional information from the structural divisions of the Company may be received by the RBM&RMD in the form of responses to specific enquiries or in the form of reports on the forms developed to analyze a specific event related to operational risks.

Each sub-type of operational risk corresponding to the Company's operational risk classification is assigned weighting coefficients (WC), depending on the degree of impact on the Company's gross income. Distribution of weighting coefficients for indicators characterizing operational risk factors is presented in the Table below.

Operational risk factors	Weight ratio, WR
external and internal fraud	0,05
labor relations	0,10
clients and business practice	0,10
failures in information and technical systems	0,10
process management	0,20
damage to fixed assets	0,10
industrial accidents	0,35
Total:	1,00

On the basis of data on the value of the risk rating and the weighting coefficient of each subspecies of operational risk, the operational risk coefficient (Kor) is calculated, which is used for further calculations. This factor is defined as the sum of the products of the risk rating value of each subspecies and the corresponding weighting factor of the operational risk factor:

Кор = ∑ (ВК i * РРi), i=1,n, where

n – total number of operational risk factors

Operational risk is calculated using the following formula:

OR = Кор*ВД*15%, where:

OR – operational risk quantification,

Kop – Operational risk ratio,

GI - The average gross income for the last three years is calculated as the ratio of the sum of annual gross income for the last three years, in each of which the Company received net income for the number of years in which the Company received net income. As long as the term of the Company's activity does not exceed three years, the average annual gross income is calculated based on the actual number of past years of activity.

Annual gross income is determined as the sum of net annual income before tax, the annual amount of allocations for the formation of provisions (reserves) and the amount of emergency expenses incurred minus the Company's emergency income.

The resulting quantitative assessment of operational risks is used to analyze the dynamics of weaknesses and strengths in operational risk management.

Regulatory values for operational risk assessment can be determined as statistics accumulate.

Operational risk is monitored by CDRD through regular analysis of information from the Risk Register and information provided by the Company's structural divisions.

Minimization of operational risk involves the implementation of a set of measures aimed at reducing the likelihood of events or circumstances leading to operational losses and the level of their impact on the Company's activities.

The main methods of minimizing operational risks are the optimization of the organizational structure and business processes, the development of internal rules and procedures for the implementation of current activities in such a way as to exclude the possibility of operational risk factors.

Reducing the financial consequences of operational risk is possible through insurance. Insurance is carried out in accordance with the Insurance Policy at Samruk-Kazyna JSC.

The risk assessment made it possible to clarify the risk map and risk significance indicators, and on this basis the critical risks of the Company are determined - those risks to which the Company should pay special attention and on which decisions on their management should be made immediately.

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

5. Normative references

№	Document title
1	Identification and risk assessment rules of Samruk-Energo JSC
2	Risk management policy of AlES JSC
3	

6. Documents and records

№	Documents and records title	Executor	Place of storage	Period of storage
1	Risks register of “AlES” JSC	CDRD	CDRD	Before the need expires
2	Risks map of “AlES” JSC	CDRD	CDRD	Before the need expires
3	Key Risk Management Action Plan Execution Report	CDRD	CDRD	Before the need expires

Annex1
(required)

Risks register of “Almaty electric stations” JSC

№	Risk passport(1)								Assessment of inherent risk (2)				
										Amount of damage			
	EC	Efficiency threshold (tolerance)	Risk code	Significant risks of not achieving strategic EC	Risk factors (causes of risk occurrence)	Description of possible consequences of risk realization	Key risk indicator	Risk owner	Probability	Impact	Damage amount in thousand tenge	Impact time	Significance score
	1	2	3	4	5	6	7	8	9	10	11	12	13
STRATEGIC RISKS (risks related to the Company's strategy)													
			Risk 1										
			Risk 2										
			Risk N										
FINANCIAL RISKS (risks related to financial activities)													
			Risk N										
Operational risks													
			Risk N										
LEGAL RISKS													
			Risk N										

Мероприятия по управлению рисками (3)						Оценка риска в результате исполнения мероприятий (4)				
							Amount of damage			
Event description	Aim	Type	Estimated cost of the event, million tenge. (specify if possible)	Event Implementation Deadline	Person/structure responsible for implementation of the event	Probability	Impact	Damage amount in thousand tenge	Impact time	Significance score Impact
14	15	16	17	18	19	20	21	22	23	24
STRATEGIC RISKS (risks related to the Company's strategy)										
FINANCIAL RISKS (risks related to financial activities)										
Operational risks										
LEGAL RISKS										

Column 15 - one of the options: A) damage reduction; B) reduced probability; C) risk prevention; D) recovery of losses.
Column 16 - one of the options for: A) risk avoidance; B) risk transfer; C) risk reduction; D) risk acceptance.

Annex 2
(referal)

Unified nomenclature for identification of main risks

Risk Number - Risk Group - Company Name in short	Full name of risk
1-C-AlES	Reputational risk
3-C- AlES	Risks of human resources of the Company
66-C- AlES	Risk of terrorist attack
8-C- AlES	Risk of damage to the health and life of employees during the performance of official duties, accidents at work.
10-C- AlES	Risks of ongoing investment projects
11-C- AlES	Social risks
29-C- AlES	Risk of corporate governance violations
55-C- AlES	Reduced electricity production
56-C- AlES	Reduction of heat energy production
15-Ф- AlES	Lack of liquidity for operating, investment and financing activities
17-Ф- AlES	Interest rate risk
18-Ф- AlES	Credit risk
24-Ф- AlES	Tariff setting
57-Ф- AlES	Increase in prices for purchased equipment, raw materials, fuel, materials and services, including infrastructure services (increase in tariffs for railway transport, communications and telecommunications, water supply, services, etc.)
65-Ф- AlES	Risk of violation of external lenders' covenants
26-O- AlES	Fraud/corruption by personnel and third parties
27-O- AlES	Leak of confidential information/use of insider information
28-O- AlES	Procurement process risks

31-O- AlES	Information systems risks
38-O- AlES	Power industry accidents and catastrophes
46-O- AlES	Technological risk
58-O- AlES	Environmental risk
59-O- AlES	Overspending of fuel for the generation of thermal and electrical energy.
60-O- AlES	Risk of poor-quality insurance protection
61-O- AlES	Facility fire
62-O- AlES	Natural disasters (avalanches, abnormally low temperatures, earthquakes, forest fires, floods, hail, abnormally high temperatures, landslides, soil subsidence, solar activity, thunderstorms (lightning strike), snowfalls, etc.
63-O- AlES	Failure to meet equipment repair deadlines
64-O- AlES	Receipt by structural divisions of goods, works and services of low quality from the supplier, contractor/contractor.
66-O- AlES	Failure of the contractor/contractor to comply with the terms of contracts, works and services
67-O- AlES	Physical damage/loss of property
48-П- AlES	Risk of tax violations
49-П- AlES	Litigation (claim work)
51-П- AlES	Risk of changes in legislation
55-П- AlES	Compliance risks
56-П- AlES	Risk of sanctions
68-П- AlES	Violation of anti-monopoly legislation requirements

Annex 3
(required)

Classification of events causing loss

Event type category (Level 1)	Definition	Category (Level 2)	Examples of activities
Inner fraud	Losses due to acts with intent to commit fraud, misappropriate property or circumvent regulations, legislation or internal regulations of the Company, with the participation of at least one internal party	Unauthorized activity	Unreported transactions (intentional) Unauthorized transaction types (resulting in monetary loss) Incorrect position valuation (intentional)
		Theft and fraud	Fraud Theft, extortion, embezzlement, robbery Assignment of assets Intentional destruction of assets Fake Smuggling Assignment of other people's accounts/use of other people's documents, etc. Intentional non-compliance with tax laws or tax evasion Bribes Insider trading (not at the expense of the Company)
External fraud	Loss due to intent to commit fraud, theft of property or violation of law involving a third party	Theft and fraud	Theft, robbery Falsification Writing unsecured checks
		System security	Hacking, theft of information, entailing monetary losses
HR Policy and Occupational Safety	Loss due to violation of labor, health and safety laws or due to payment of personal injury or discrimination claims	Employee Relations	Pay, compensation and severance issues Organization of labor activity
		Safe environment	General accident liabilities
		Discrimination	All types of discrimination
		Personnel qualification	Insufficient qualification of personnel
Customers, products and business practices	Loss due to inadvertent negligence in the performance of professional obligations towards specific customers (including trust and qualification requirements) or due to	Acceptability, disclosure, fiduciary relationship	Breach of fiduciary relationship/breach of instructions Disclosure issues (know your customer) Breach of disclosure requirements to retail customers. Violations related to the disclosure of confidential personal

	the nature or design of the product		information. Aggressive sales Artificially inflated fees Abuse of confidential information Lender's obligations
		Improper business or market practices	Antitrust laws Poor trading/market practices Market manipulation Insider trading Activities without license Money laundering
		Product flaws	Product defects Design errors
		Selection, sponsorship and risk	Failure to comply with customer study requirements Exceeding risk limits per customer
		Consulting services	Disagreements in estimates of consulting services
Damage to physical assets	Loss due to damage to physical assets due to natural disasters or other events	Disasters and other events	Damage from natural disasters, human losses from external sources (terrorism, vandalism)
Business irregularities and system failures	Losses due to business and system failures	Systems	Software Hardware Telecommunications Power and utility failures
Execution, Delivery and Process Management	Losses due to disruption of transaction processing or process failures or due to relationships with trading counterparties and sellers	Execution and maintenance of operations	Incorrect communications, errors when entering, loading or maintaining data Violation of deadlines or obligations Incorrect functioning of systems or models accounting errors/errors in counterparty attribution Other task errors Delivery disruption Breakdowns in collateral management Maintenance of reference data
		Monitoring and reporting	Non-compliance with mandatory reporting Inaccurate external reporting resulting in losses
		Customer acquisition and documentation	Lack of permits/release of liability from customers Missing or incomplete legal documentation
		Manage customer accounts	Unauthorized account access Incorrect customer records resulting in loss

			Customer damages or losses resulting from negligence
		Trading counterparties	Incorrect actions of counterparties Conflicts with counterparties
		Suppliers and contractors	Outsourcing Conflicts with suppliers

Annex 4
(required)

Risk Management Action Plan Execution Report

№	Risk code	Risk name	Event name	Aim	Type	Estimated cost of the event, million tenge. (specify if possible)	Event Implementation Deadline	Person/structure responsible for implementation of the event	Event Execution Status	Residual Risk Significance Score	Assessment of the effectiveness of the event
1	2	3	4	5	6	7	8	9	10	11	12
STRATEGIC RISKS (risks related to the Company's strategy)											
FINANCIAL RISKS (risks related to financial activities)											
OPERATIONAL RISKS											
LEGAL RISKS											

Column 5: one of the options: A) damage reduction; B) reduced probability; C) risk prevention; D) recovery of losses.
Column 6: one of the options for: A) risk avoidance; B) risk transfer; C) risk reduction; D) risk acceptance.
Column 11:1 - effective, 0 - ineffective

Annex 5
(required)

RISK IDENTIFICATION QUESTIONNAIRE

Date of completion:
Full name of employee:
Structural subdivision:
1 - Perform SWOT analysis in the area of activity of your structural subdivision, indicating: **a) strong intrinsic factors (Strengths);** **b) external factors representing opportunity (Opportunities);** **c) weak intrinsic factors (Weaknesses);** **d) external threat factors (Threats)**

Strong points:	**Weak point:**
Opportunities:	**Threats:**

2 - Based on the SWOT analysis, determine the main risks that have a negative impact on the achievement of strategic goals by your structural unit.

Risk №1	
Risk №2	
Risk №3	

3 - Identify risk factors (reasons) for each risk identified in paragraph 2.

Risk №1	1	
	2	
	3	
Risk №2	1	
	2	
	3	

Annex 6
(required)

RISKS QUESTIONNAIRE

№	Name of the risk	The Company's exposure to risk	If YES, evaluate the probability, impact, time of risk impact by ticking the appropriate checkbox		
			Frequency or probability of risk	Effects of risk	Time of risk impact
1		☐ yes ☐ no	☐ Once every 7 years or more (or probability of occurrence up to 5%)	☐ No consequences in case of risk realization	☐ There's time to fix
			☐ Every 5 years (or probability of occurrence up to 25%)	☐ The consequences of risk realization are not significant	☐ Risk impact manifests with time lag
			☐ Once every 3 years or more (or probability of occurrence up to 40%)	☐ The consequences of risk realization are not significant and can be fully corrected	☐ Risk manifests with immediate effect
			☐ Once a year (or 80% probability)	☐ The consequences of risk realization are very significant, but can be corrected to a certain extent	
			☐ Every six months or more (or more than 95% chance)	☐ If the risk is realized, the company will practically not be able to recover from the consequences associated with this risk	
2		☐ yes ☐ no	☐ Once every 7 years or more (or probability of occurrence up to 5%)	☐ No consequences in case of risk realization	☐ There's time to fix
			☐ Every 5 years (or probability of occurrence up to 25%)	☐ The consequences of risk realization are not significant	☐ Risk impact manifests with time lag
			☐ Once every 3 years or more (or probability of occurrence up to 40%)	☐ The consequences of risk realization are not significant and can be fully corrected	☐ Risk manifests with immediate effect
			☐ Once a year (or 80% probability)	☐ The consequences of risk realization are very significant, but can be corrected to a certain extent	
			☐ Every six months or more (or more than 95% chance)	☐ If the risk is realized, the company will practically not be able to recover from the consequences associated with this risk	

Annex 7
(required)

RISKS QUESTIONNAIRE
(annual interviewing)

1. What risks were realized over the past calendar year in your division that led to losses (fines, lost profits, additional expenses, etc.)?

2. What risks were realized over the past calendar year in your division that led to a negative effect (impact on the Company's reputation, overdue control orders, etc.)?

3. What risks can affect the achievement of goals and objectives for your department?

4. What risks are most likely to be realized that will affect the achievement of goals and objectives for your department?

5. What risks are inherent in the activities of your division that may affect the achievement of the Company's strategic goals?

6. What negative effects can occur when risks (events) occur in your unit, and what is the possible amount of damage?

7. What measures will be taken to mitigate the risk, i.e. to reduce the likelihood of negative events or damage from a possible risk or negative event?