Annex No.2
to the decision of the
Management Board of
Samruk-Kazyna JSC
of _____, 2025
Minutes No.____

CORPORATE STANDARD ON PROCESS SAFETY MANAGEMENT FOR THE SAMRUK-KAZYNA JSC GROUP

Version: 2.0
Owner: H&S Sector
Developer: H&S Sector

Astana, 2025

Table of Contents

Section 1. Purpose and General Provisions

1. The main purpose of the Corporate Standard on Process safety management for the Samruk-Kazyna JSC Group (hereinafter - the Corporate Standard) is to provide unified regulatory and methodological support for issues within the framework of building/improving the occupational safety management system of Samruk–Kazyna JSC (hereinafter - the Fund) and its portfolio companies, taking into account legislative requirements of the Republic of Kazakhstan, the best international practices and approaches, as well as the specifics of the Fund's portfolio companies

2. The requirements of this Corporate Standard are established in accordance with the requirements of the legislation of the Republic of Kazakhstan in the field of labor protection, transportation occupational safety, industrial, fire, radiation, nuclear safety, etc., fully comply with them and are an addition to them. The need to improve the current occupational safety management system is related to the importance of safety, accident and injury prevention, and the introduction of modern proactive models and tools in occupational safety management that ensure planning, solving, and tracking the following tasks:

1) achieving a highly organized occupational safety system, where the company operates without interruptions, as the number of malfunctions, downtime, and quality issues with products and services are reduced;

2) enhancing occupational safety culture and employee engagement at all levels;

3) implementing a systems approach to occupational safety management that is simple, transparent, and understandable at all levels;

4) a preventative management approach aimed at preventing incidents, injuries, and occupational diseases;

5) proactively identifying hazardous actions and conditions to reduce the number of incidents, accidents, and accidents, as well as the scale of their consequences (damage);

6) ensuring unified approaches to ensure compliance with applicable legislative and other occupational safety requirements, unified data management, and the elimination of duplication;

7) organizing a systemic analysis of the root causes of accidents and cases of occupational diseases, the causes of accidents and incidents, hazardous conditions and hazardous actions, as well as cases of violation of regulatory requirements;

8) ensuring rational planning and implementation of measures to create favorable and safe working conditions and promptly eliminate non-compliance with regulatory requirements;

9) ensuring the reliable operation of hazardous production facilities in accordance with regulatory operating requirements and the risk management system;

10) ensuring the effectiveness of industrial control and the implementation of an

integrated approach to its implementation at all levels, detailed monitoring and analysis of occupational safety processes;

11) ensuring coordination of employee actions and awareness in the area of occupational safety.

Section 2. Scope of Regulation

3. This Corporate Standard applies to the occupational safety management system in portfolio companies of Samruk-Kazyna JSC (hereinafter - the Fund) engaged in industrial activities. The Corporate Standard is mandatory for implementation by the Fund and its portfolio companies in the area of occupational safety.

Section 3. Terms and Definitions

4. The following terms and definitions are used in this Corporate Standard:

1) **Root cause analysis (RCA)** - a structured, step-by-step process that helps identify the main factors or causes of an adverse event. Understanding the factors contributing to a system failure, or the causes that cause it, helps to develop a response plan to fix the problem and avoid it in the future;

2) **Hazard and Operability Study (HAZOP) -** a systematic qualitative methodology for identifying technological hazards and potential operational problems by using a set of keywords (guide words) to analyze deviations from design intentions. The HAZOP method is used for a thorough and step-by-step analysis of each element of the process in order to identify possible deviations, their causes and consequences. This technique is suitable for both continuous and batch processes and can be used for both new and existing installations;

3) **Life-Saving Rules** - the key requirements for the safe performance of work, developed on the basis of international best practices in the field of occupational safety of leading companies, as well as the analysis of available information about accidents, incidents and accidents in the Group of Companies;

4) **Lagging indicators** - indicators for assessing the extent and actual consequences in the risk management system, reflecting one or more obstacles (barriers) at the same time;

5) **Process Safety Information (PSI)** – a set of technical, design, operational and other engineering information necessary for hazard identification, risk assessment and ensuring the safe operation of hazardous production facilities. It includes information about chemicals and materials used in the process; information about the technological process; data on the design, construction and technical condition of equipment; drawings (PFD, P&ID, BFD); automation and emergency protection

(including the Cause-Effect Matrix), as well as other documentation related to the provision of occupational safety;

6) **Safety observation card/Hazard observation card)** – a tool that allows employees of PCs and contractors to report unsafe working conditions, actions, behavior, and potentially dangerous cases at facilities, as well as to make proposals to reduce the impact of hazardous and harmful production factors, improve working conditions, the condition of equipment, buildings, structures, and the mechanisms and tools used during work, which is a fundamental element of preventive measures for risk management in the field of occupational safety;

7) **Key performance indicators (hereinafter - KPI)** - a fundamental element in the process of evaluating the performance of managers. KPI is an indicator that characterizes the degree to which goals are achieved;

8) **Motor Vehicle Crash Rate, MVCR** - the number of traffic accidents in the last 12 months multiplied by 1 million km and divided by the mileage traveled (in the last 12 months);

9) **Fatality Accident Rate, FAR** - the number of people injured in fatal accidents over the past 12 months multiplied by 100 million man-hours and divided by the total number of man-hours worked (over the past 12 months);

10) **Lost Time Injury Frequency, LTIF** - the number of injured (including those died) in disability accidents over the past 12 months multiplied by 1 million man-hours and divided by the total number of man-hours worked (over the past 12 months);

11) **Root (main) causes** – factors related to management, such as deficiencies in the management system that influenced the occurrence of an accident or incident;

12) **Corrective Measure** - an action taken to eliminate the cause of an identified nonconformity or other undesirable situation and prevent its recurrence;

13) **Crisis Situations -** an unplanned disruption of the normal functioning of the PC, endangering the stability of its activities; an incident that can have a significant impact on the PC reputation, its financial well-being or viability in the long term;

14) **Safety Culture -** a set of characteristics and features of the activities of organizations and the behavior of individuals, which establishes that OS issues, as having the highest priority, are given attention determined by their significance;

15) **Safety Measures -** planned specific activities of an organization aimed at fulfilling the goals in the field of OS, determined by the requirements of legislative and other regulatory legal acts, including the organization's policy and internal regulatory documentation;

16) **Microtrauma -** a FAC, First Aid Case, limited to one-time treatment and subsequent examination of minor scratches, cuts, burns, splinters, etc., which does not entail medical care or a more serious injury;

17) **Vision Zero** - an approach to prevention that combines three areas -safety, occupational health and the well-being of workers at all levels of production;

18) **Hazard -** an industrial factor that can cause injury or other harm to human

health;

19) **Leading Indicators -** indicators for assessing the extent and actual consequences in the risk management system, reflecting the effectiveness in maintaining the risk management system;

20) **Major Accident Hazards MAH** - represent potential sources of serious incidents that can lead to significant consequences for human health and life, the environment, equipment, and/or the reputation of the company. MAH includes scenarios that may result in serious injury, death of personnel, release of hazardous substances, major fire, explosion, structural failure, or other events beyond the normal operational risk;

21) **Behavioral Audits/Surveillance/Safety Dialogues (SBA/SBS/SBD) -** an observation in which managers of all levels, specialists of all categories, representatives of employees and employees of OS services visit production facilities, places of work, observe the actions of employees and discuss hazardous or safe working methods and involve employees in active compliance with the OS requirements;

22) **Contractor -** a legal entity or an individual who performs work, renders services or supplies inventory items on the territory or in the interests of the Fund PC in accordance with a contract (agreement) and which may affect the OS quality;

23) **OS indicators - indicators characterizing the PC activities in the field of OS**;

24) **Near Miss** – an incident that did not cause injury or damage;

25) **Proactive Tools (methods) -** an approach aimed at improving the safety culture, as well as at anticipating the manifestation of negative consequences on workers and the environment, through prompt and targeted elimination;

26) **Occupational Safety (OS) -** a management system that includes processes in the field of occupational & health safety, industrial and fire safety, as key areas and radiation, nuclear safety, electrical safety, transportation occupational safety, etc., as specific processes of individual PCs;

27) **Accident -** any unplanned event that occurred as a result of or during the production activity of a PC, which led or could lead to an accident related to work, to a fire, explosion, accident, incident or failure, a traffic accident or any other event that has an impact on the business and reputation of the PC;

28) **Occupational Disease -** an acute or chronic disease caused by the exposure of an employee to harmful production factors in connection with the performance of their work (official) duties.

29) **Risk** - a combination of the probability of occurrence of a hazardous event in the course of work, the severity of injury or other damage to human health caused by this event;

30) **Physical Cause -** a malfunction or a change in the quality of the equipment, or when the physical condition of the equipment leads to undesirable consequences. As

an example, the following situations can be cited: pipeline rupture/leakage, pump vibration, malfunction of the heat sensor, formation of carbon deposits on the furnace pipes, lightning entering the tank, or a short circuit of the electrical wiring;

31) **Human Factor -** a human action or inaction that caused an undesirable physical condition or action.

Section 4. Basic Principles and Approaches

5. Basic principles of OS management are as follows:

1) **Management leadership -** managers create unity of goals of the company and management, demonstrate commitment to principles on OS issues, create and maintain an internal environment in which employees could be fully involved in achieving the company's goals;

2) **Employee engagement -** employees at all levels form the basis of the production process, full involvement makes it possible to effectively use their abilities to improve the safety culture;

3) **Systematic approach -** the efficiency and performance of OS are improved by defining, understanding and managing a system of interrelated processes in accordance with established goals;

4) **Risk-based decision-making -** effective decisions are based on a proactive analysis of data and incoming information;

5) **Continuous improvement** - continuous improvement should be an ongoing goal of OS management to improve operations and ensure benefits.

6. Persons responsible for organizing the OS management system should be senior managers directly reporting to the CEO of the company.

7. For the effective and efficient functioning of the OS management system, it is necessary to train and certify personnel of various categories according to legal requirements and internal procedures. Staff training should be continuous, step-by-step, and include basic training for both managers, starting with their senior management, and employees of departments according to applicable system requirements.

8. Along with the training, the staff is constantly informed and familiarized with the goals and tasks in the field of OS.

9. Confirmation of the high-quality functioning of the OS management system is the availability of standards, procedures, instructions, manuals and other documents that describe the processes necessary for functioning of the OS management system. The scale and depth of the procedures are determined depending on the size and type of production, the complexity and interconnection of processes, methods used, as well as qualifications and degree of staff training involved in the work.

10. For organizing the OS management activities in the Company, the principle of a process approach is applied, including processes of the management system, implementation of senior management responsibilities (defining strategies and goals, planning company activities and resources), resource management (HR, infrastructure and production environment), measurement, analysis and improvement.

11. In the effective OS management system, processes are established and maintained in a consistent manner:

1) Responsible persons for processes are appointed;
2) Procedures and techniques related to it are documented;
3) Necessary resources are identified and the processes are coordinated;
4) Their interrelationships are determined;
5) Their compatibility is ensured.

12. Functioning of the system ensures transparency, manageability, development, competitiveness of production activities, and must also comply with the Plan-Do-Check-Act cycle and include the following areas:

1) Planning of the OS management system;
2) Functioning of the OS management system;
3) Monitoring and analysis of the OS management system;
4) Subsequent improvement of the OS management system.

13. Relevant approaches are being established to achieve the main tasks of the Fund in the field of OS management:

1) Promote best practices in the field of OS and show commitment to the Zero Traumatism concept;

2) Act in strict accordance with the national legislation of the Republic of Kazakhstan, develop and improve the internal/local requirements of the Fund companies based on the best international practices. Take ESG principles into account when planning and implementing safety measures, including environmental impact assessment, employee well-being and corporate ethics, and accountability;

3) Maintain an effective OS management system in PCs and contribute to the growth of employee engagement and improvement of safety culture;

4) Ensure development and financing of measures aimed at improving the safety of specific production processes and creating healthy and safe working conditions in the Fund PCs;

5) Maintain effective monitoring and control systems for the state of working conditions and occupational safety in the workplace, prevention and localization of emergency situations;

6) Improve the OS management system and promote the use by PCs, contractors and related organizations of the same principles defined in this corporate standard;

7) Apply proactive tools to increase the OS level, such as registration and investigation of hazardous conditions, hazardous actions and potentially hazardous

incidents Near Miss, conducting Behavioral Audits/ Observations/Safety Dialogues, using safety monitoring/event registration cards, exercising the right to stop unsafe work conditions, and more;

8) Ensure the necessary safety measures for workers and the public in the area of production facilities in accordance with current legislation;

9) Develop and improve the technical equipment, structure and level of training of operational personnel of organizations, formations serving high-risk facilities, warning and emergency response systems to reduce and control the level of the risk of accidents and emergencies at production facilities;

10) Establish a unified procedure for recording and investigating industrial accidents, including cases of occupational diseases, as well as events affecting the safety of facilities;

11) Ensure the application and operation of digital, automated, information OS systems;

12) Improve the qualification of specialists - develop the professional skills of personnel in the field of OS;

13) Ensure the safety and hygiene of workplaces;

14) Motivate employees by involving them in solving OS issues together with management;

15) Develop and implement programs to achieve goals and take concrete steps;

16) Ensure the protection of the health of employees by prioritizing the life and health of employees in relation to the company's activities;

17) Increase transparency and develop a culture of free expression of employees about incidents, hazardous conditions, hazardous actions and potentially hazardous incidents Near Miss in the field of OS.

14. The application of above-mentioned approaches is minimal and can be expanded by a decision of the PC management. These approaches are necessary to increase the efficiency of the OS management system, which will allow achieving a qualitative improvement in the safety culture, reducing injuries and accidents.

Section 5. Business Processes

15. Processes of occupational safety management are based on the following:

1) **Occupational safety.**

Description: recognize and ensure the priority of preserving the life and health of employees in relation to the results of production activities. The principle provides for implementation by the management of a OS policy, stimulating the creation of healthy and safe working conditions, introduction of safe technologies, use of personal and collective protection equipment, and participation in priority financing of OS measures.

Value: application of this principle will make it possible to increase the priority

of OS issues and form an approach in which economic benefit will not be of primary interest when it comes to OS.

2) **Unification and establishment of uniform OS requirements for all production companies of the Fund.**

Description: Manage OS activities, including supervision and compliance control, including the use of advanced automated/digitalized technologies for a unified management system. The principle is based on the standardization of approaches to OS, optimization of all management procedures and reporting, guarantees of transparency and comparability of information received from all companies of the Fund.

Value: the use of a unified, automated/ digitalized approach will allow to take decisions quickly, save money on the coordination and control over all OS activities.

3) **Risk-based approach to the organizing and planning of activities.**

Description: it strives to achieve OS through managing and controlling the amount of acceptable risk. The principle is based on the acceptance of the minimum amount of risk that is achievable through technical, economic and technological capabilities. The amount of acceptable risk depends on the type of industry, profession, and the type of negative factor that determines it.

Value: the use of a risk-based approach, subject to economic opportunities, will improve the safety of technical systems, reduce acceptable risk and ensure the continuity of production activities. The level of acceptable risk is achieved as a result of optimizing the cost of investments in the technical, technological and social sphere of production.

4) **Awareness of employees about the state of working conditions and labor protection.**

Description: it is necessary to achieve a positive effect, influence on the discipline and mood of employees by involving employees through providing timely feedback, as well as increasing their awareness, forming a safety culture. The principle is based on the dissemination of advanced domestic and foreign experience in improving working conditions, working out information about accidents, including industrial accidents.

Value: increase employee loyalty, increase efficiency and quality of work, increase safety culture. The involvement of each employee in the implementation of OS measures and the system of continuous identification and elimination of hazards and risks.

5) **Regular planning and monitoring of planned OS indicators.**

Description: achieving corporate and social responsibility and goals, increasing production efficiency through the assessment and control over OS indicators at all levels in the Fund companies.

The principle is based on preventive planning and reduction of the number of violations and hazardous OS behavior by employees, commitment to the OS policy, as well as ensuring continuous improvement through compliance with legislation,

proactive management methods and high speed of decision-making and control over decisions execution.

Value: increasing the efficiency of the used complex of organizational and technical measures in planning by maximizing the return and payback of invested funds.

6) **Compliance with applicable requirements.**

Description: reducing the risks of non-compliance with standards, technical and regulatory acts in force on the territory of the Republic of Kazakhstan. The principle is based on achieving compliance and adaptation of business processes when legislation changes.

Value: increasing the degree of compliance, reducing the occurrence of risks and penalties, reducing the risk of accidents.

7) **Ensuring the completeness, transparency and reliability of information.**

Description: transparency of the information provided, including through digitalized technologies with the appointment of a responsible person for the completeness and reliability of the information.

The principle is based on increasing the level of awareness of management and employees through promptly providing information in a convenient format for taking operational decisions.

Value: increasing the efficiency of process management.

Section 6. Process Description

16. Methodologically, the OS management system is based on principles of international standards such as ISO 45001, ISO 31010, etc., recommended for use in the Republic of Kazakhstan and permits to conduct activities in the field of OS using state, industry and local requirements.

17. OS processes include management system planning, management system functioning, management system monitoring, management system efficiency analysis, including regulatory requirements tracking, production control, inspections and other processes that ensure compliance of activities with applicable requirements.

Planning of the OS Management System

18. Planning of OS activities shall be carried out by:

1) Formation of an OS policy and development of OS goals;
2) Identification and risk assessment;
3) Identification of legal and other applicable OS requirements;
4) Development of OS measures.

Management's Responsibility

19. Management undertakes the following obligations to confirm its leadership

and ensure the effectiveness and efficiency of the OS management system:

1) Leadership - assuming overall responsibility for the prevention of injury and deterioration of health, as well as providing safe and healthy workplaces and activities;

2) Development of the mission, vision, values and strategic goals of the company;

3) Development of policies and OS goals as well as their periodic monitoring, discussion and adjustments;

4) Communicating the Policy and OS goals to each employee, achieving universal understanding and support for the set goals and tasks;

5) Bringing the importance of meeting the OS requirements, as a personal responsibility of each employee to the attention of the staff;

6) Provision of the organizational structure and resources necessary to maintain the OS management system in working order;

7) Timely financing of work on the creation, implementation and development of the OS management system;

8) Conducting an analysis of the OS management system by the management and taking measures to improve it;

9) Creating an environment contributing to employee engagement in the management of OS processes and procedures;

10) Continuous staff training at all levels of management of the organization, improving their skills and business qualities;

11) Increasing staff motivation;

12) Ensuring the efficient and effective functioning of the OS management system and its continuous improvement.

20. Managers at all levels, within their competence, are responsible for managing and involving employees in the process of achieving goals and fulfilling OS tasks. This is achieved in the following ways:

1) Managers are an example of behavior, demonstrate commitment to OS issues by their personal example, form and encourage a positive attitude of employees towards OS issues;

2) A manager maintains open and effective interaction with employees;

3) Each manager improves their skills and knowledge in the field of OS in the process of training and practical work;

4) Managers ensure the exchange of information on OS issues with employees, contractors and other persons, including through meetings, regular monitoring of compliance with the requirements of the OS management system in the workplace, and open discussion of OS issues with employees;

5) Managers formulate clear goals and OS tasks, assign responsibilities and areas of responsibility, define performance criteria, allocate the necessary resources;

6) The OS activities of managers are assessed on the basis of their fulfillment of annual target indicators in this area;

7) Managers promote the dissemination of OS experience, demonstrate support for OS processes;

8) Managers are responsible for organizing the risk management process in the field of OS in their subdivisions;

9) Managers create working conditions that allow any employee to demand that work be stopped if its continuation poses a hazard to employees and people around them;

10) Managers ensure continuous improvement of existing OS practices and procedures.

Policy Formation and Goals Development

21. The OS management system in the company ensures the development and implementation of the company OS Policy, followed by the development of goals based on legitimate and socially responsible business and commercial activities.

22. The OS Policy is an equal and consistent part of strategic goals of the company.

23. The Policy management procedure includes: development, coordination, approval of the Policy, communication to staff, updating, analysis and, if necessary, making changes.

24. Supreme management ensures that Policies are understood, implemented and supported at all levels.

25. The Policy is implemented using the OS management system, which sets goals, tasks and procedures for the performance of work, distribution of responsibilities and authorities, allocation of resources, including providing of qualified personnel, constant monitoring of the organization's processes and analysis of the system functioning as a whole.

26. Policy analysis for relevance, continued suitability and compliance with goals is carried out annually, as well as when strategic goals change.

OS Goals

27. The main requirements for building the structure of the OS management system, ensuring effective goal setting:

1) Apply a systematic approach to OS management aimed at identifying risks and their effective control;

2) Promote best OS practices;

3) Apply proactive injury reduction tools;

4) Ensure the preservation of the life and health of employees, as well as to promote a healthy lifestyle;

5) Ensure compliance with OS as a factor of sustainable development of the company;

6) Implement advanced digitalized OS management software technologies;

7) Delineate functions at all levels;

8) Carry out direct and feedback communications of all management units;

9) Improve qualifications - develop professional skills.

28. Goals, tasks and measures for their implementation are formed on the basis of requirements of the OS Policy, identified and assessed hazards and risks, as well as proposals from heads of subdivisions, subject to allocated resources, including the opinions of stakeholders (employees, contractors, customers and companies engaged in similar activities).

29. In accordance with the OS Policy and based on initial or subsequent analyses of the OS system functioning, measurable OS goals should be established, which should be:

1) specific to the organization, as well as acceptable and appropriate to its size and nature of activity;

2) consistent with requirements of relevant and applicable national laws and regulations, as well as with the technical and commercial obligations of the organization related to OS;

3) aimed at the continuous improvement of protective measures and the Zero Traumatism achievement;

4) realistic and achievable;

5) documented and brought to all relevant functional structures and PC levels;

6) periodically evaluated and updated if necessary.

30. The OS Action Plan is developed annually, which specifies the tasks set to improve the safety culture and perform safe work.

31. The Report on completing tasks is sent within the time limits set by the Action Plan.

31-1. Information on the implementation of the Action Plan on a monthly or quarterly basis (as decided by the Fund) is provided by the responsible persons of the Fund's portfolio companies through the Samruk App digital platform.

31-2. Specialists from the H&S sector of the Fund monitor the progress of the Plan's activities through the Samruk App digital platform on a monthly basis or once a quarter (according to the Fund's decision).

32. The achievement of goals and the fulfillment of OS tasks is regularly, but at least once a quarter; it is monitored and analyzed by management.

33. When analyzing, the management should put emphasis on:

1) deadline for completion;

2) quality of execution;

3) progress of execution;

4) sufficient funding, if necessary.

Identification and Assessment of OS Risks

34. Identification of OS risks is an ongoing process that determines the past, present and potential impact of PC activities on occupational safety. When planning, all types of PC activities are considered, as well as operations performed by contracting

organizations and other contractors, persons, in accordance with concluded contracts, based on the OS requirements when performing certain types of work/services.

35. Identification of hazard sources during systematic inspection of production operations makes it possible to identify risks to the life and health of workers, production facilities and equipment.

36. Prioritization of OS risks is carried out subject to results of their assessment, as well as the impact on human health, equipment condition, reputation and activities of the company.

37. It is necessary to plan a systematic review of results of the hazard sources identification, assessment and prioritization of risks.

38. Risk management permits to achieve the following OS goals:

1) Creating a more complete, accurate and correct basis for decision-making and planning;
2) Ensuring more reliable identification of hazards and potential threats;
3) Estimating the uncertainty and variability of OS-affecting processes;
4) Preventive elimination of sources of hazardous events;
5) More efficient allocation and use of resources;
6) Improving the management of potentially hazardous incidents;
7) Ensuring compliance with legal and other applicable requirements;
8) Improving the OS management system;
9) Increasing the OS level.

39. Stages of risk management are divided into:

1) Identification of hazards;
2) Risk assessment;
3) Development of risk management measures;
4) Implementation of the developed measures;
5) Control over the measures.

Identification of Hazards

40. The source of information (the basis) for identification of hazards are:

1) regulatory and technical acts, standards in force on the territory of the Republic of Kazakhstan, as well as internal regulatory documents of the PCs;
2) results of inspections of supervisory and controlling state bodies of the Republic of Kazakhstan;
3) results of production control over OS;
4) results of the production facilities certification according to working conditions;
5) results of monitoring the technological process, production environment, workplace, work of contractors, external factors;
6) results of the analysis of questionnaires, inquiry schedules;
7) results of occupational safety state audits;
8) risk assessment registries;

9) proactive tools (behavioral safety audits, identification and accounting of potentially hazardous incidents, microtraumas, etc.);

10) statistical data and analysis of injuries and accidents;

11) circumstances of incidents and accidents that occurred in the PC or similar industries.

41. Sources of OS hazard in accordance with the hierarchy of control measures are subject to (in order of decreasing their effectiveness):

1) deleting;

2) replacing;

3) managing;

4) control;

5) providing personal and collective protective equipment.

Risk Assessment

42. Risk assessment refers to determining the magnitude and significance of emerging risks based on early identified hazards. Risk assessment includes the establishment of probabilistic (frequency) characteristics and severity indicators. Risk assessment is the most effective preventive measure. When assessing risks, not only adverse events and accidents that occurred earlier are taken into account, but also hazards that have not yet caused adverse consequences.

43. Risk assessment is a continuous and systematic process and permits to identify hazards before they cause an accident or cause other harm.

44. Informed decisions can be taken to improve the level of safety based on the risk assessment. In order for the risk assessment to really result in improvements, it is necessary to determine priority measures based on the data obtained. The most effective measures include measures to completely eliminate the most apparent hazards. The proposed measures should be specific and feasible.

45. Risk assessment is carried out according to the risk matrix under the set process in companies.

46. Results of the risk assessment and the risk management measures developed are used as input data when compiling OS work plans.

47. The main goal of the risk assessment process is a detailed study of what can harm personnel, facility, environment or PC reputation, conducted in such a way that it is possible to weigh whether enough management measures have been implemented and what exactly should be done to prevent possible undesirable consequences.

47-1. Unified risk assessment methodology

To ensure comparability, transparency and manageability of risk analysis approaches in all divisions and organizations of the Fund's Group, it is necessary to develop, approve and apply a unified corporate methodological approach to risk assessment in the field of occupational safety.

The methodology should include:

– a scale of severity of the consequences (by category: health and life of personnel, equipment and infrastructure, environment, reputation and business sustainability);
– a scale of probability or frequency of occurrence of events;
– classification of risk levels (high, medium, low), including graphical representation in the form of a risk matrix;
– criteria for risk acceptability and required actions (e.g. risk acceptance, corrective measures, suspension of work);
– a description of the process of documenting the risk assessment, requirements for the composition and registration of records, as well as the procedure for reviewing previously conducted assessments (based on the results of incidents, changes, audits, etc.).

This methodology is mandatory for:
– identification and assessment of risks within the framework of the PB system;
– when implementing the change management process;
– when developing action plans to reduce risks;
– during the planning and implementation of projects in the hazardous production facility.

47.2 Formation of key risk scenarios

For systemic risk management with a high level of potential consequences, as well as to support emergency response planning, hazard analysis, and investment support for safety measures, organizations are required to develop and keep up-to-date key risk scenarios for all facilities with high residual risk.

Each scenario should include:
– identified hazard and source of occurrence (e.g. substance, energy, operational error);
– possible triggering events and escalation triggers;
– affected equipment or site, including process chains and systems;
– impact zones (personnel, infrastructure, environment, reputation);
– existing protective barriers (technical, organizational) and assessment of their reliability;
– description of possible consequences in case of failure of barriers (including destruction, injury, emissions, production shutdown, etc.).
Scenario format requirements:
– a single document form (according to a template);
– assigning a unique identifier and linking it to an object and equipment;
– integration of scenarios with HAZOP, LOPA, IRP, MOC and investment planning systems.

Scenarios should be reviewed at least once every 3 years or when the following events occur:
– implementation of MOC changes;
– accident, incident or serious Near Miss;
– decommissioning/commissioning of equipment;

– the emergence of new data on the effectiveness of protective barriers.

47-3. Assessment of sufficiency and reliability of protective barriers

When analyzing significant risks and forming key risk scenarios, the organization is required to assess the adequacy and reliability of existing protective barriers to prevent and/or mitigate the consequences of dangerous events.

The approach should include:

– identification of all existing barriers within the considered scenario;

– classification of barriers: technical (engineering), procedural (administrative), behavioral (depending on the actions of personnel);

– assessment of the independence of barriers (IEC/LOPA-compliant principle): barriers should not depend on a single triggering event or failure channel;

– assessment of the reliability of barriers (for example, by the probability of failure on demand – PFDavg, response time, support/maintenance);

– calculation of the residual risk after the application of all existing barriers.

The specified approach is applied:

– when developing and updating key risk scenarios;

– when managing significant changes (MOC);

– when analyzing incidents with ineffective or failed protection;

– when forming investment plans and justifying CAPEX/OPEX measures to increase the level of security.

Development of Risk Management Measures

48. When developing measures, it is necessary to be guided by requirements of the legislation of the Republic of Kazakhstan, internal documents that are applicable to a specific risk and hazard.

49. Risk management measures being developed should be feasible subject to time, financial, labor, technical, legal and organizational constraints.

50. The list of activities includes subordinate activities, for each of which the following is given:

1) Risk name;
2) Facility (material, unit of equipment, technical location, etc.);
3) Legal and regulatory requirements;
4) Management tools (measures to reduce risks);
5) Resources;
6) Responsible person;
7) Deadline for completion;
8) Mark on completion.

Implementation of the Developed Measures

51. Implementation of the developed measures is necessary to reduce risks.

52. Control over implementation of the measures is carried out by the designated

person responsible for measure implementation.

53. When performing, it is necessary to understand the problem as a whole, assessing the effectiveness of the implemented risk reducing measures.

54. Implementation of measures is not limited to the available resources to reduce risk.

Control over the Measures

55. The goal of the control is to evaluate the completed activities and changes in the situation.

56. Through regular monitoring, it is necessary to monitor changes in risk levels, the emergence of new risks, as well as the degree of effectiveness of measures taken.

57. The need for control depends on:

1) the magnitude of a risk level;

2) resources at disposal;

3) changes, completed activities.

Identification of Legal and Other Applicable Requirements

58. In their OS activities, the Fund PCs are guided by legislative requirements, regulatory documents, standards in force on the territory of the Republic of Kazakhstan, as well as internal regulatory documents (hereinafter - IRDs) (technological regulations, instructions, plans of organizational and technical measures, orders, instructions, etc.).

59. Compliance monitoring of the company's activities with legislative and other applicable requirements includes:

1) identification and registration of legislative and other OS requirements, which apply to the PC activities;

2) monitoring changes in existing requirements of legislation and regulatory OS documents, as well as the emergence of new requirements;

3) access of PC personnel to legislative and other OS requirements;

4) OS performance evaluation of the company for compliance with legislative and other requirements.

60. Main sources of information for monitoring the compliance of PC activities with the requirements of legislative and other documents include:

1) regulatory, legal and technical acts, standards in force on the territory of the Republic of Kazakhstan and other applicable OS requirements;

2) technological regulations (operation charts);

3) requirements of state supervision and control bodies;

4) results of inspections and implementation of OS measures;

5) registers of hazards and risks of the company;

6) results of certification of production facilities, etc.

61. Based on the PC's OS performance evaluation in accordance with

requirements of regulatory and legal documents, in case of non-compliance, measures (corrective, preventive actions) are developed.

OS Measures

62. Measures are records of planned actions that need to be performed in connection with the risk assessment carried out, implementation of best practices, need to comply with legislative requirements, IRDs, as well as due to received acts and regulations.

63. Planning of OS measures includes:

1) development, coordination and approval of programs as part of the OS management system;

2) development and implementation of annual OS action plans, including occupational safety and health, industrial and fire safety.

64. Planning is based on:

1) requirements of the legislation of the Republic of Kazakhstan and international OS requirements ratified in the Republic of Kazakhstan;

2) PC strategies and internal OS requirements;

3) legal requirements of public authorities;

4) results of the risk assessments carried out;

5) results of the examination of technical devices, certification of production facilities;

6) environmental monitoring results;

7) analysis of the root causes of accidents, violations of rules and regulations, accidents and occupational diseases, emergencies;

8) analysis of the state of labor protection and health conditions of employees;

9) analysis of results of the implementation of previous programs to improve the OS Management System;

10) analysis of results of the implementation of annual OS action plans.

65. Measures are divided into operational and planned ones.

66. Operational measures include tasks that are developed as part of an accident or when critical risks are identified.

67. Planned activities are tasks included in OS programs or annual action plans to improve working conditions, etc.

68. Measures classification as part of control measures is divided into:

1) organizational measures that include:

- distribution of responsibilities and authorities of employees who directly perform operations related to OS risks or manage the execution of such operations;
- training of employees in OS risk management measures, etc.;
- development of procedures (including documented ones) with established criteria for performing operations related to OS risks;
- development and implementation of emergency response procedures;

- OS audits;
- etc.

2) Technical measures that include:

- replacing hazardous technologies or hazardous substances with safe ones;
- design and implementation of safe technologies;
- inhibition and other ways to protect pipelines, production facilities and equipment;
- use of modern transport;
- use of collective protection equipment and equipment that ensure OS and safe working conditions for employees;
- technical and technological measures aimed at ensuring the integrity and occupational safety of equipment and technical devices, reducing emissions, discharges, reducing waste generation and disposal;
- preventive and scheduled inspections and repairs of equipment;
- etc.;

69. The following factors are taken into account when planning measures to reduce OS risks:

1) technical feasibility of risk reduction measures;
2) expected degree of risk reduction;
3) costs related to activities implementation.

70. When planning OS activities, target indicators for use of proactive tools should be set.

71. The main attributes of measure planning include:

1) Name;
2) Facility (material, unit of equipment, technical location, document, etc.);
3) Resources;
4) Responsible person;
5) Desired result;
6) Deadline for completion;
7) Mark on completion.

72. The PC annually develops OS action plans. These annual action plans are developed before the start of the planned year and in accordance with the existing financial planning system. All subdivisions related to the OS management process should participate in the development of targeted OS action plans.

73. The estimated amount of costs to ensure implementation of the OS action plan is included in the PC draft budget for the coming and subsequent years.

6.2 Functioning of the OS Management System

Training on OS Issues. Motivation and Staff Encouragement

74. The OS management system provides for ensuring the proper competence of

PC staff based on appropriate education, training, skills and experience.

75. In order to manage the training process and develop staff competencies, it is necessary to identify the need for the necessary competencies and subsequent training related to OS risk management, legislative requirements and best international practices for staff training and subsequent evaluation of the training effectiveness.

76. Activities related to the training and maintenance of staff competence include:

1) Setting requirements for the staff competence;

2) Selection and staff placement in accordance with the approved organizational structure and staffing table;

3) Determination of the need to improve the staff competence based on requests from heads of subdivisions subject to the following factors:

- Mandatory legal requirements;
- End of the certification period for professions and positions controlled/supervised by public authorities;
- Change of functions as part of the OS processes, introduction of new rules and other requirements;
- Introduction of new equipment and technology, results of external and internal audits, etc.;

4) Risk assessment and analysis of information on identified inconsistencies, violations, hazardous actions, hazardous conditions;

5) Competence improvement planning;

6) Staff awareness of the role and importance of their activities, ways to achieve OS goals;

7) Analysis and evaluation of the effectiveness of measures taken to achieve the required competence;

8) Organization of work on the certification of employees performing certain types of OS activities;

9) Keeping records of education, training, skills and experience.

77. The process of learning, developing competencies and skills in the field of OS should be a continuous process and aimed at all levels of the PC.

78. Training and OS knowledge testing of employees is carried out in accordance with the current legislation of the Republic of Kazakhstan and best practices.

79. Persons who are hired, as well as employees who are transferred to another position, are trained, followed by a OS knowledge test, within the time limits set by the employer, but no later than one month after conclusion of an employment contract or transfer to another job.

80. Employees who have not been trained and tested on OS issues are not permitted to work.

81. OS training (classes, lectures, seminars) is conducted by the employer with the involvement of highly qualified specialists from relevant industries, engineering

and technical workers with at least three years of work experience, technical inspectors on labor protection, OS services of the PC itself, as well as specialized organizations.

82. The training programs on OS issues provide theoretical and industrial training, considering the specifics of this organization.

83. Industrial training on OS issues, safe working methods and techniques is carried out in classrooms, workshops, sites, workshops under the guidance of responsible employees of the organization for occupational safety.

84. OS training of employees ends with a knowledge test (exam, test).

85. Results of examining the knowledge of employees are compiled in accordance with the current legislation of the Republic of Kazakhstan.

86. If an employee receives an unsatisfactory assessment, a re-examination of knowledge is appointed within the time limits established by the legislation of the Republic of Kazakhstan or IRDs. The employee undergoes repeated training and is suspended from work in accordance with the procedure provided for by the current legislation of the Republic of Kazakhstan.

87. Motivation and staff encouragement to maintain an appropriate OS culture is an integral element of the personnel training system.

88. The goals of motivating and staff encouraging as part of a particular program include:

1) Improving the quality of production tasks;

2) Strengthening responsibility for violation of the OS requirements;

3) Remuneration of employees for the achieved results of OS activities (material / non-material type of bonus);

4) Increasing the interest of employees in the proper performance of their work duties, compliance with OS requirements and improvement of the OS system.

88-1. Staff involvement in the processes of ensuring industrial safety.

The program of employee involvement in ensuring industrial safety. For the formation of a mature safety culture and the effective functioning of the safety management system in the organization, an Employee Engagement Program should be developed and implemented. The purpose of the program is to ensure the systematic participation of employees at all levels in the processes of ensuring and improving safety, including identifying hazards, taking initiatives, participating in analysis and decision-making.

The program should include:

– goals and principles of engagement (openness, transparency, mutual trust);
– forms of employee participation in PB processes (participation in HAZOP, RCA, behavioral audits, safety committees, working groups);
– tools for collecting initiatives and feedback (observation cards, digital platforms, suggestion boxes, surveys);
– the procedure for non-material and/or material incentives for active participation and submission of initiatives implemented with a positive effect;

– indicators of the effectiveness of engagement (for example, the reach of staff, the number and effectiveness of initiatives, feedback on the results of the review).

88-2. Development of competencies and retention of key personnel in the field of industrial process safety management

The program for the development and retention of competent personnel in the field of industrial process safety management (IPSM).

For the sustainable functioning of the IPSM system and the preservation of corporate expertise, it is necessary to implement a Program for the development and retention of competent personnel aimed at ensuring continuity, motivation and professional growth of employees involved in the PB processes.

The program should include the following components:

Career Development Map:

– setting the levels of professional growth (beginner → specialist → expert → leader → mentor);

– definition of transition criteria: length of service, certification, participation in key events (HAZOP, etc.);

– designation of the approximate time for mastering each level.

Targeted appointments and mentoring:

– appointment of mentors from among experienced specialists;

– participation of promising employees in digitalization projects, the introduction of new approaches and risk management tools.

Motivation and recognition:

– non-material and/or financial incentives for passing the stages of development;

– allocation of the status of “OS Expert” in the structure of subsections with expanded powers and participation in corporate initiatives.

Contracts with trained specialists (as decided by the employer):

– the possibility of securing employees after corporate training on key topics (HAZOP, etc.) through agreements of intent or employment contracts.

Monitoring and feedback:

– analysis of the reasons for dismissals of trained personnel;

– regular clarification of the program content based on feedback and the needs of the organization.

Incident Management

89. All incidents that fall under requirements of legislative and regulatory acts in the field of OS in the Republic of Kazakhstan are investigated in strict accordance with these requirements. In addition, it is recommended to analyze the root causes of hazardous conditions, hazardous actions, potentially hazardous incidents, microtraumas, gross violations of OS requirements.

90. As each incident is a sign of a failure of the PC control system, and not only physical failures or human errors, it is recommended to conduct internal investigations in order to determine the root causes of the incidents (please see an example of the

applicable methodology in Annex 1).

91. The main task of the root cause identification system is to prevent the recurrence of incidents.

92. The process of determining the root causes through logical analysis should track all cause-and-effect relationships in order to identify key factors related to management systems (system errors). This will permit to focus on improving management systems (procedures, job functions and responsibilities, controls and staff training, work processes).

93. In general, the root cause identification process contributes to the continuous improvement of the safety management system by:

1) Determining conditions that may cause accidents in the future;

2) Developing and implementing measures to prevent the recurrence of accidents;

3) Developing and improving policies, procedures, guidelines and standards.

Accident and Emergency Preparedness

94. The OS management system should include the process of identifying and analyzing potential emergencies, as well as planning for mitigation and incident control. Operational response plans should be kept up-to-date in order to carry out operational actions, if necessary.

95. Accident and emergency management consists in analyzing potentially serious incidents that can have a significant negative impact on the PC operation in normal mode, and developing measures to prevent and/or mitigate their consequences.

96. It is necessary to identify any possible unplanned events and, as part of the risk management plan, companies should define procedures for responding to accidents and emergencies.

97. PCs should provide for the procedure of actions of the staff/employees of contractors in responding to accidents and emergencies.

98. Preparedness for and response to accidents and emergencies is ensured by:

1) Planning of measures to identify, prevent, limit and eliminate the consequences of accidents and emergencies;

2) Training of employees/staff, including contractors, in the event of accidents and emergencies (scheduling of training alarms and training sessions, creation of a committee (teams) for crisis management, creation of emergency response headquarters at different levels, emergency training and development of actions in case of a conditional occurrence of an accident, etc.);

3) Providing appropriate means for the localization and elimination of accidents and emergencies;

4) Availability and operability of communication systems, etc.

99. Accident and emergency action plans should cover (but not be limited to):

1) Organization, responsibilities, authorities and procedures for emergency

response, including support for internal and external communications;

2) Systems and procedures for providing personnel with shelter, evacuation, rescue and treatment;

3) Systems and procedures for preventing, mitigating and monitoring the consequences of emergency actions;

4) Procedure for communication with the authorities, relatives and other stakeholders;

5) Systems and procedures for the mobilization of equipment, company premises and staff;

6) Measures and procedures for mobilizing third-party resources for emergency support;

7) Procedure for notifying the local population falling into the zone of impact of accidents and emergencies;

8) Measures and procedures for training response teams and testing emergency systems.

100. The main goal of emergency response is to minimize any negative risks, prevent the escalation of accidents and emergencies at a time of crisis, and prepare staff for actions during accidents and emergencies.

101. To assess the effectiveness of response plans, the company must maintain procedures for verifying action plans in case of accidents and emergencies by working out scenarios, conducting training alarms and emergency training in accordance with the current legislation of the Republic of Kazakhstan. At the same time, not limited to requirements of the legislation.

Lean Equipment Maintenance Management System

101-1. The purpose of the process of implementing a lean equipment maintenance management system, according to Annex No. 2, is to increase the level of occupational safety, reliability and efficiency of production processes through optimal equipment condition management.

101-2. The main objectives of implementing a lean equipment maintenance management system are:

1) ensuring reliable and safe operation of equipment at all production facilities;

2) reducing equipment downtime related to emergencies;

3) involving employees in the autonomous service process;

4) development and implementation of preventive measures to prevent malfunctions.

101-3. The fundamental elements of the lean equipment maintenance management system are:

1) involve all employees, including equipment operators, technical staff, and management in improvement processes;

2) autonomous maintenance involving operators in the daily maintenance of

equipment, including visual diagnostics, cleaning, lubrication, minor repairs and the use of checklists to monitor its condition;

3) focusing on eliminating six main types of losses, such as: downtime due to breakdowns, changeover and reconfiguration losses, losses due to short-term shutdowns or slow operation, product defects and repeated alterations, losses at the start of production, unnecessary maintenance losses;

4) development of an equipment maintenance schedule to prevent breakdowns and extend its service life;

5) implementation of small but regular improvements aimed at increasing equipment efficiency (Kaizen method);

6) training employees with the knowledge and skills necessary to effectively interact with the equipment and implement improvements;

7) monitoring of equipment performance indicators, which includes three key aspects: availability (downtime), productivity (speed of execution) and quality (percentage of products meeting the requirements);

8) creation of a safe and favorable working environment, providing for the maintenance of cleanliness, order and safety in the workplace, with the introduction of the 5S system (Sort, Set in order, Shine, Standardize, Sustain).

101-4. The advantages of creating a lean equipment maintenance management system are:

1) reducing the number of accidents at work;

2) reducing the number of accidents and incidents;

3) lower equipment repair costs;

4) raising workers' awareness of the need to comply with occupational safetystandards;

5) formation of a systematic approach to occupational safetymanagement at production facilities;

6) prolonging the service life of the equipment.

101-5. The implementation of a lean equipment maintenance management system implies a clear distribution of roles and responsibilities at all levels of the organization:

1. The heads of structural divisions and workshops provide overall guidance and control over the implementation of lean equipment maintenance management programs, monitor the implementation of equipment maintenance plans and maintenance schedules, organize interaction between divisions and promote employee involvement in the processes of maintaining equipment in working order.

2. Equipment operators perform autonomous maintenance, including daily inspections, cleaning, lubrication, and troubleshooting, promptly identify and report any equipment malfunctions, and participate in self-care training.

3. Occupational safety specialists identify and account for the risks associated with the operation of equipment, develop recommendations for eliminating potential

hazards, audit the technical condition of the equipment, train employees on the principles of safe operation and participate in the analysis of the causes of malfunctions, developing measures to prevent them.

4. Maintenance services ensure that scheduled and unscheduled repairs are carried out, maintain equipment maintenance documentation, and cooperate with operators to promptly eliminate malfunctions.

101-6. The implementation of the lean equipment maintenance management system provides for the realization of a long-term program that includes diagnostics of the current condition of equipment, training of employees in lean maintenance methods, development and implementation of maintenance procedures, as well as continuous process improvement to improve the efficiency, reliability of equipment and safety of equipment operation.

Contracting Organizations Management

102. This process applies to all contractors who perform work and render services for PCs.

103. When classifying the risk degree related to performance of works/services under a certain agreement (contract), the following factors should be taken into account:

1) Possible consequences or impact of their activities on the PC activities;
2) Type/ nature of the work performed;
3) Place of work;
4) Type/nature of the risk factor;
5) Duration of work performed/services rendering;
6) Contractor's experience and competence to perform work/render services;
7) Probability of an accident risk for contractor staff that performs work/renders services or PC workers;
8) Probability of an accident and/or emergency as a result of the contractor's activities on the territory/facility of the company.

104. It is necessary to be guided, but not limited to, the following approaches when interacting with contractors:

1) OS requirements imposed on the contractor must comply with requirements imposed on the PC itself;
2) Appointment of an administrator of the agreement (contract), who is responsible for the completeness of providing information in order to comply with OS requirements when performing works/rendering services under the contract by the contractor;
3) After conclusion of the contract, before the start of rendering services and performing work by employees of the contractor, preparatory measures are carried out for admission to the PC territory / facility with verification of permits, standards, internal regulatory documents in the field of OS;

4) Inspections of work of a contractor performing work/rendering services should be carried out at least once a quarter or more often, in the presence of serious incidents;

5) In all contracts for works performing/ services rendering by contractors on the PC territory / facility or in the PC interests to provide liability for violation of the OS requirements;

6) Develop and apply the interaction procedure and requirements for contractors on the PC territory / facility;

7) Conduct training and familiarize employees of contractors with risks and hazards of the company, in those places/areas where employees will perform work/render services on the PC territory/ facility;

8) Familiarize employees of contractors with their actions in the event of accidents and emergencies in accordance with accident response plans.

105. OS information for familiarization of employees of contractors should be publicly available on the company's website.

106. The main goal of the process is to define clear responsibilities, ensure active interaction with contractors, and also propose a consistent program for managing OS issues, which permits to prevent incidents in contractors related to OS violations.

Operational Activities and Change Management

107. The goal of establishing requirements for the operational activities is to ensure manageable conditions when performing production processes, including production and technological operations and types of activities.

108. The production processes (operations and activities) management provides for the development and implementation of the necessary documentation as the basis of the production process and the OS management system.

109. The production process is carried out under controlled conditions, which include:

1) Availability of information describing the features of the production process (GOSTs, standards, technical specifications);

2) Ensuring compliance of equipment, premises and workplaces with the OS requirements;

3) Creation of infrastructure and production environment;

4) Staff training;

5) Submitting necessary documentation, including procedural documents;

6) Operational and calendar planning;

7) Strict compliance with parameters of the production process and OS;

8) Availability and application of control and measuring devices;

9) Monitoring and measurements;

10) Correction of processes and procedures in case of deviations from the established OS requirements.

110. All processes that have a significant impact on OS must be evaluated through consistent monitoring and measurements.

110-1. Change management is aimed at ensuring safety during the implementation of technical, technological, organizational and other changes that may affect production processes, equipment, personnel or the level of risk.

The change management process includes:

– initiating a change with a description of the essence and reason;

– preliminary identification of hazards and risk assessment prior to implementation;

– review and approval of changes with the participation of responsible specialists (including technologists, engineers of OS, H&S, ecology, operation, design, etc.);

– determining the need for an official risk analysis (for example, HAZOP);

– updating process safety information (hereinafter - PSI), procedures, instructions and training materials;

– carrying out the necessary training and informing the staff before the changes are put into effect;

– documenting and monitoring the implementation of the change;

– monitoring the effectiveness of the change and, if necessary, corrective actions.

For all permanent and temporary changes, a formalized approval procedure should be applied, with mandatory registration in the change log and/or the digital change management system.

110-2. Classification of changes by level of significance

For the purposes of effective change management, a classification of changes is established according to the level of their potential impact on the safety of production processes:

– Highly significant changes are changes that can affect high-risk facilities (HRF), MAH scenario prevention systems, basic technological parameters, emergency protection, management systems, personnel health, environmental protection, as well as changes initiated in response to accidents, accidents, or regulations from supervisory authorities.

– Medium—significant changes - changes affecting work procedures, secondary equipment, personnel without interfering with critical technological or protective functions.

– Minor changes are administrative, organizational, or documentary changes that do not affect the level of risk.

Each change should be classified at the initiation stage with its level of significance recorded.

Depending on the level of significance, an appropriate assessment procedure is applied:

– for highly significant changes, an official risk assessment (HAZOP, LOPA, etc.) is required;

— for medium–significant changes, a basic assessment with an expert opinion;

– for minor changes, a simplified verification of compliance with the OS requirements.

All changes are recorded in the change management journal (or digital register) indicating the classification, date, responsible person, results of the risk assessment and the status of implementation.

110-3. Risk assessment when initiating changes

Any change related to technical, technological, organizational, personnel and other aspects of production activities is subject to mandatory preliminary risk assessment before its implementation.

The preliminary risk assessment process should include:

– identification of new or increased hazards arising from the proposed change;

– quantitative and/or qualitative risk assessment using a risk assessment matrix approved by the organization;

– documenting the results of the assessment, indicating the residual risk and proposed measures to reduce it;

– involvement of specialized specialists (in the field of technology, safety, occupational safety, ecology, operation, design, etc.) for a comprehensive expert assessment.

If there is a high potential level of risk or if critical equipment, process chains, security systems, control system, or MAH facilities are affected, formalized hazard analysis methods (for example, HAZOP) should be used.

The risk assessment should be completed before the change is approved, and its results should be used when deciding whether the change is acceptable, whether additional measures are needed, and whether related documentation (including PSI, instructions, response plans, etc. should be updated.).

110-4. Revision of the risk assessment in case of changes

When implementing any changes affecting production processes, equipment, personnel, management structure, or documentation, it is imperative to review identified hazards and previously performed risk assessments.

The review includes:

– checking the relevance of existing hazards, risks, and scenarios;

– analysis of the possible impact of the change on existing protective barriers, technological parameters, and operating conditions;

– assessment of the need to adjust current risk management measures;

– determining the need for a new analysis (for example, HAZOP) depending on the level of significance of the change;

– documentation of the revision results and integration into the risk assessment register.

The risk review must be completed prior to the approval and implementation of the change and is included in the mandatory list of steps for approval within the framework of the change management system.

The results of the revision should be used for updating:

– process safety documentation;

– operational instructions;

– action plans for OS and staff training.

110-5. Documentation and management of information on the safety of production processes (PSI)

In order to ensure effective identification of hazards, risk assessment, change management and staff training, an organization must establish and maintain an up-to-date information management system on the safety of production processes (PSI).

The information should include (but not be limited to):

– flow charts: PFD, P&ID, BFD;

– technical characteristics and specifications of the equipment;

– material safety data sheets (MSDS);

– descriptions of technological modes and critical parameters;

– philosophy of management and automation, logic of protection, C&E-matrix;

– energy and material balances;

– narratives on installations, lists of protective barriers and response systems.

The organization is obliged to:

– assign responsible persons for maintaining, updating and controlling access to PSI;

– provide centralized digital storage of PSI documents with version control and change tracking capabilities;

– ensure access to the PSI database for all participants in the processes related to risk assessment, MOC, HAZOP, operation, training and incident investigation;

– ensure that PSI is reviewed and updated after changes, accidents, corrective actions, or scheduled technical revisions are implemented.

The availability of up-to-date, reliable and accessible process safety information is a prerequisite for the functioning of the safety management system.

Proactive OS Management Tools

111. Proactive tools are needed to identify and respond to hazards, risks, register safety proposals, engage and inform employees.

112. Examples of proactive tools include:

1) Identification, registration, investigation of hazardous conditions, hazardous actions, potentially hazardous incidents;

2) Application of behavioral dialogues/audits/safety observations;

3) Introduction of the stopping unsafe types of work practice;

4) Use of Safety Observation Card/ Hazard Observation Card for safety

monitoring (submission of proposals for improvement and reports on hazards at work);

5) etc.

113. It is necessary to involve both PC workers, visitors, and employees of contractors in the process of using proactive tools.

114. All PC workers and contractors should have access to the use of proactive tools.

115. In order to involve PC employees, use available economic and social means to encourage and motivate, guarantee anonymity, if necessary, and not put pressure on the employee.

116. To maintain the performance of proactive tools, it is necessary to apply (but not limited to) the following minimum solutions:

1) Realization of the right to use a proactive tool, including through digital technologies;

2) Realization of the right to stop unsafe work and implementation of risk prevention measures;

3) Feedback on the specific fact of using a proactive tool;

4) Analysis and monitoring of the use of proactive tools by PC managers and employees.

Processes Digitization

117. In order to implement effective solutions, the use of digital OS solutions is recommended.

118. Digitalization is the main factor in increasing the efficiency and productivity of the process, as well as reducing the cost of the OS management function.

119. Digitalization of OS management processes permits:

1) Effectively manage the process on the ground by quickly analyzing and raising staff awareness;

2) Increase the speed of decision-making and reduce operating costs;

3) Prevent and reduce the number of incidents and inconsistencies;

4) Ensure transparency and control over processes;

5) Guarantee a systematic approach and contribute to the continuous improvement of indicators;

6) Provide information in a way that is convenient for decision-making;

7) Promptly monitor and manage changes;

8) Proactively manage risks;

9) Enter data once and receive notifications;

10) Generate reports promptly;

11) Effectively analyze existing trends of detected violations, inconsistencies, hazardous actions, hazardous conditions.

Communication with Stakeholders

120. The existence of effective communication processes in the field of OS implies informing employees in the form of internal and external communication, participation in the stakeholders' OS management, and consulting on OS issues.

121. This process defines approaches in the field of information exchange by:

1) Reporting the management's position and expectations on OS issues;

2) Warning about existing hazards and risks;

3) Sharing the best OS practices;

4) Clarification of the OS requirements to employees;

5) Involvement of employees in the work on OS improvements.

122. Existing methods of propaganda influence can be divided into two groups:

1) Single-channel communications, when there is an impact channel, but there is no direct feedback channel to control the perception of this impact. The means of single-channel exposure include:

- printed publications (brochures, information sheets, etc.);
- safety posters, wall newspapers;
- safety alerts;
- information stands and corners on OS;
- exhibitions, lectures and reports;
- audiovisual media (TV, cinema, filmstrips, radio broadcasts, etc.).

2) two-channel communication, in which it is possible to control its perception in the process of exposure. Two-channel impact is realized through the organization of:

- the system of safety committees and subcommittees at various levels of companies;
- collective discussion with workers of accidents, ways of injury prevention, etc.

123. Work in this direction should be aimed at the following results:

1) development and improvement of the current communication system to achieve a higher level of positive motivation for safe work;

2) creation of a communication plan and tools for bringing information to employees and back from employees to the management of enterprises;

3) establishment of vertical and horizontal corporate communications aimed at openly informing employees on OS issues.

124. Vertical information exchange permits to bring goals and tasks to the attention of employees. Also, this exchange provides an opportunity for employees to make suggestions on OS improving, to bring an opinion on working conditions to the attention of management.

125. The horizontal exchange of information is aimed at coordinating the interaction of employees of the PS structural subdivisions and subsidiaries in order to achieve the common OS tasks.

126. Employees of organizations give suggestions:

1) on safe working methods and necessary measures to improve working conditions;

2) on defining the OS needs and expectations;

3) on defining mechanisms for fulfilling the OS requirements;

4) on setting OS goals and on planning measures to achieve them;

5) on defining indicators for OS monitoring and evaluation;

6) on establishing audit objects;

7) on determining directions for improving OS activities.

127. The head or his/her OS representative brings the necessary information about possibilities of their participation in the OS management system improving to the employees.

128. Communication with stakeholders is carried out in order to comply with principles of openness and accessibility of OS indicators, declared in the Policy being formed.

129. Consulting and participation of employees in the development, maintenance

and improvement of the OS management system is ensured by their involvement in the following types of OS work:

1) Determining mechanisms for consultation, training and participation;

Identifying hazards and OS risk assessment, determination of applicable management measures to eliminate hazards and reduce OS risks;

2) Developing proposals to improve the OS effectiveness;

3) Defining competence requirements, training needs;

4) Defining OS communication needs and communication methods;

5) Defining OS management measures and their effective application;

6) Investigating OS incidents and identifying causes of inconsistencies, participation in the development of Accident Prevention Action Plans and Corrective Action Plans.

6.3 OS Monitoring and Effectiveness Analysis

Monitoring

130. The basic requirements for the OS management system are based on regular and unscheduled monitoring of activities to ensure the implementation of OS measures, improvement of working conditions of employees, including contractors/subcontractors, including periodic monitoring of parameters of harmful and dangerous factors of the production environment that can cause significant harm to staff health.

131. The goals of the monitoring process include:

1) Control over implementation of OS programs and plans;

2) Improving working conditions;

3) Reducing the adverse effects of harmful and hazardous production factors on

the staff health;

4) Prevention and minimization of accidents;

5) Monitoring the timely conduct of emergency and fire prevention training;

6) Safety of production processes at hazardous production facilities;

7) Timely identification of hazards and associated risks;

8) Analysis and evaluation of OS indicators, effectiveness of production and other management tools and methods.

132. It is necessary to implement (but not limited to) the following activities as part of the monitoring:

1) Comprehensive and target OS inspections;

2) Periodic monitoring of parameters of harmful and hazardous factors of the production environment;

3) Verification of compliance with requirements for the safe performance of work by PC workers and contractors;

4) Verification of the correctness of organizing and conducting on-the-job briefings to employees, including contractors;

5) Control over training, checking the quality of assimilation of OS knowledge;

6) Control over implementation of measures to eliminate inconsistencies recorded in the regulations of the supervisory authorities;

7) Control over the technical condition of equipment, technical devices, buildings and structures;

8) Workplace safety control;

9) Control over the availability and condition of primary fire extinguishing equipment;

10) Control over the condition and correct use of personal protective equipment (PPE) and collective protection by employees of the company, as well as employees of contractors;

11) Control over the sanitary condition of household and auxiliary premises;

12) Control over compliance with OS regulations at night, on weekends and holidays;

13) Control over facilities under construction and reconstruction;

14) Organization and participation in the certification of production facilities as part of legislative and regulatory requirements;

15) Organization and participation in the identification of hazards and risks in order to minimize them;

16) Control over implementation of corrective measures as part of the root cause analysis.

132-1. As part of the control and monitoring of the implementation of measures to eliminate the causes of accidents, the following actions are carried out:

1) Based on the results of special and internal accident investigations, specialists from the portfolio companies of the Fund enter corrective measures into the SAP

Business Objects Planning and Consolidation (hereinafter – SAP BPC) information system, indicating the deadlines for implementation and the persons responsible;

2) The experts in the Health and Safety Sector of the Fund monitor the progress of the measures on a monthly basis using SAP BPC, checking the deadlines, completeness, and accuracy of the data provided;

3) Portfolio companies are responsible for timely implementation of corrective measures. The Health and Safety Sector of the Fund provides methodological support, summarizes information and monitors compliance with deadlines and quality of implementation;

4) Information on the progress of measures implementation is used in analyzing the effectiveness of the occupational safety management system, preparing reports, and planning corrective and preventive measures at the Fund level.

133. OS monitoring is used for the current assessment of the effectiveness and efficiency of OS activities, improvement of working conditions of employees, prevention of failures/incidents, accidents, injuries and occupational diseases. All of these activities are based on the hazards and risks identified in the subdivisions. A program for achieving goals and solving OS tasks is being formed on the basis of hazards and risks registers.

134. To implement the procedure for monitoring operations and activities affecting OS, a program is being compiled to achieve OS goals and tasks.

135. The program for achieving goals and OS tasks includes the fulfillment of requirements and OS measures.

136. The following are recognized as nonconformities:

1) failure to comply with requirements of legislation, regulatory and technical documentation, as well as IRDs;

2) failure to comply with requirements of instructions, regulations;

3) failure to comply with orders, instructions, and information letters brought to the attention of;

4) failure to implement planned measures to eliminate inconsistencies recorded in the regulations of the supervisory services and inspection organizations;

137. Monitoring results are used in the analysis of the OS management system by management.

OS Effectiveness Analysis

138. Companies use a systematic approach to analyzing their OS activities on a regular basis.

139. As part of the management analysis, the PC considers the following at least once a quarter:

1) the level of safety culture;

2) information on results of the implementation of commitments reflected in policies, programs and plans to achieve goals and solve problems in order to improve;

3) levels of exposure to harmful factors to determine whether the relevant legal requirements, as well as other requirements, have been violated;

4) incidents that have occurred;

5) information on the implementation of key performance indicators (KPIs) of the organization in the field of OS;

6) analysis of the resources sufficiency (financial, labor, material and technical resources, etc.) to fulfill the stated obligations;

7) analysis of the use of proactive incident tools;

8) the value of the Fatality Accident Rate - the number of injured persons in fatal accidents related to work x 100 000 000 man-hours / number of hours worked during the reporting period;

9) the value of the severe injury coefficient - the number of seriously injured persons in work-related accidents × 1 000 000 man-hours / number of hours worked during the reporting period;

10) the value of the Lost Time Injury Frequency - the number of injured persons in accidents with disability related to work (including those who died) × 1 000 000 man-hours / number of hours worked during the reporting period;

11) the OS state report in contractors, including the values of the Fatality Accident Rate, the Lost Time Injury Frequency rate, the severe injury rate, information on violations, accidents, inspections by public authorities, etc.);

12) results of the work of branches/subsidiaries of the organization;

13) results of consideration of OS-related complaints and appeals from public organizations, the public and other stakeholders.

140. The results of the analysis should be used by the senior management of the companies in the Fund to assess opportunities for improving the OS Management System and the need for changes, including amendments to OS policies, objectives, and programs.

141. In order to motivate PCs to improve occupational safety management systems, the “Procedure for Remuneration of Portfolio Companies with an Annual Nomination of the Chief Executive Officer of Samruk-Kazyna JSC for Achieving Results in the Field of Occupational Safety” has been defined, in accordance with Annex No. 4.

141-1. In order to foster personal involvement of CEOs in occupational safety issues, strengthen the role of management in developing a safety culture, and increase employee motivation, the Fund organizes an annual nomination for “The Most Involved CEO in Occupational Safety Issues” among the portfolio companies of Samruk-Kazyna JSC in accordance with Annex No. 5.

Key performance indicators for management processes

142. KPI is the basis for managing the efficiency of OS processes. KPIs should be a driver of efficiency and correspond to the strategic goals of the company. The OS

management process should be evaluated based on the KPIs recommended below:

Key performance indicators used in companies:

POSITION	KEY PERFORMANCE INDICATORS (KPI)
CEO and his/her Deputies in the following areas	The LTIF coefficient (Lost Time Injury Frequency) in relation to the indicator of the previous year Introduction and analysis of the effectiveness of corporate standards according to the annual plan Timeliness of financing of OS risk management activities Introduction of proactive management processes/tools
Heads and Deputies of structural subdivisions	Development of organizational and technical measures based on results of the root causes of accidents identification reports Timely and complete annual planning of financial costs for OS activities Conducting a certain number of behavioral security audits in a subordinate subdivision and the actions taken
Line managers (head of installation, site)	Identification and registration of potentially hazardous incidents Proposals for improving the OS management system Implementation of measures to improve the OS management system

143. The listed KPIs are minimum requirements and are not exhaustive, but only set directions for the development of specific KPIs that reflect the business characteristics of each PC individually.

143-1. Companies should establish occupational safety targets for managers of structural subdivisions who are administrators of agreements with contractors.

6.4 Methodology for conducting cross-functional/internal audits

144. Goals and objectives

The goal of conducting cross-functional (internal) audits is as follows:

1) prevention of emergencies, accidents, fires, incidents;

2) identification and prevention of violations in occupational health and safety, industrial and fire safety, as well as in related areas, including radiation and nuclear safety, electrical safety, transport safety, and others, depending on the specific activities of individual PCs;

3) ensuring uniform approaches to occupational safety management within the group of companies, including the assessment of the management system for PPE, protective clothing and footwear, and first aid kits, including the processes of their accounting, distribution, updating, and quality control;

4) exchange of best practices between the portfolio companies of the Fund;

5) monitoring the effectiveness of previously adopted corrective measures;

6) development of professional competencies of occupational safety specialists;

7) improvement of the safety management system in the field of occupational health and safety, industrial and fire safety.

145. Principles of conduct and professional ethics for auditors

In order to ensure high quality, objectivity, and trust in the audit results, all participants in the audits are required to adhere to the following principles:

1) ethical conduct - adherence to moral and professional standards, respectful and correct behavior, avoidance of biased and unethical decisions or actions;

2) integrity and trust - truthfulness, adherence to principles, sincerity, and fulfillment of obligations to both colleagues and the audited party;

3) confidentiality, non-disclosure, and protection of information obtained during the audit;

4) impartiality – the duty to present accurate and objective results without distortion;

5) professional diligence – the application of common sense, experience, and accuracy in gathering and analyzing information;

6) independence – exclusion of conflicts of interest, independence from external influence when forming conclusions;

7) evidence-based approach – forming conclusions based solely on verifiable facts and evidence.

146. Justification of the approach.

Conducting cross-functional/internal audits with the participation of specialists from other portfolio companies of the Fund allows:

1) to ensure independent and objective assessment of the state of occupational safety management systems;

2) to identify hidden or recurring system failures;

3) to promote internal corporate interaction and professional exchange of experience.

147. Participants of cross-functional/internal audits

The cross-functional/internal audit committee shall include:

1) representatives of the Health and Safety Sector of the Fund;

2) occupational safety specialists of the portfolio companies of the Fund;

3) specialists from the Center for Young Workers on Occupational Safety of the group of companies of the Fund and other young specialists from the group of companies of the Fund.

148. Criteria for selecting audit objects

Scheduled cross-functional/internal audits are conducted in accordance with the approved annual schedule. The schedule for cross-functional and internal audits is drawn up annually, taking into account the following priorities:

1) Subsidiaries/Branches where fatalities were registered;

2) Subsidiaries/Branches where severe accidents were registered;

3) Subsidiaries/Branches where accidents with injuries to employees that were not fatal and/or serious were most frequently registered;

4) other Subsidiaries/Branches.

Depending on the specifics, the PC must ensure maximum coverage of audits of Subsidiaries/Branches during the calendar year.

149. Audit stages

1) Preparation stage

- defining the Subsidiary/Branch;
- agreeing on the audit schedule;
- forming the audit team;
- appointing contact persons on the part of the audited organization.

2) Planning

- drafting an audit program with distribution of areas and zones of responsibility among commission members;
- preparation of verification sheets, checklists, and other supporting documentation.

3) Conducting an audit

Before the audit begins, the following is carried out:

- introductory meeting with the management of the audited Subsidiary/Branch, during which the objectives, format, timing, and procedure of the audit are explained;
- briefing for all commission members, including an explanation of potential hazards on the site, requirements for the use of personal protective equipment, rules of conduct in emergency situations, as well as information on movement routes and restricted access areas.
- during the audit, production facilities and technical infrastructure are inspected, regulatory and organizational documentation is analyzed, employees are interviewed, and any violations identified are recorded in photographs and videos. In doing so, the commission members are required to comply with the legislation of the Republic of Kazakhstan and the internal regulatory documents of the portfolio company under audit.

150. Members of the cross-functional/internal audit committee are entitled to:

1) unhindered access to the territory and premises of the inspected facility in compliance with the requirements of the access control and internal facility regime;

2) receive documents (information) on paper and electronic media or copies thereof for attachment to the audit report, as well as access to automated databases

(information systems) in accordance with the subject of the audit;

3) take audio, photo, and video recordings;

4) use recordings from technical surveillance and recording devices, photo and video equipment related to the subject of the audit.

151. The results of the audit shall be recorded in the Occupational Safety Audit Report in the form provided in Annex 3.

151-1. The Occupational Safety Audit Report shall be drawn up in duplicate at the site of the inspection and signed by the chair of the commission (or his/her deputy), all members of the commission, and the CEO of the inspected organization or an authorized representative. If the inspected party disagrees with the content of the report, a dissenting opinion shall be recorded in the report.

152. The results are discussed at a final meeting, after which one copy of the Occupational Safety Audit Report is given to the audited party and the other remains with the Health and Safety Sector of the Fund.

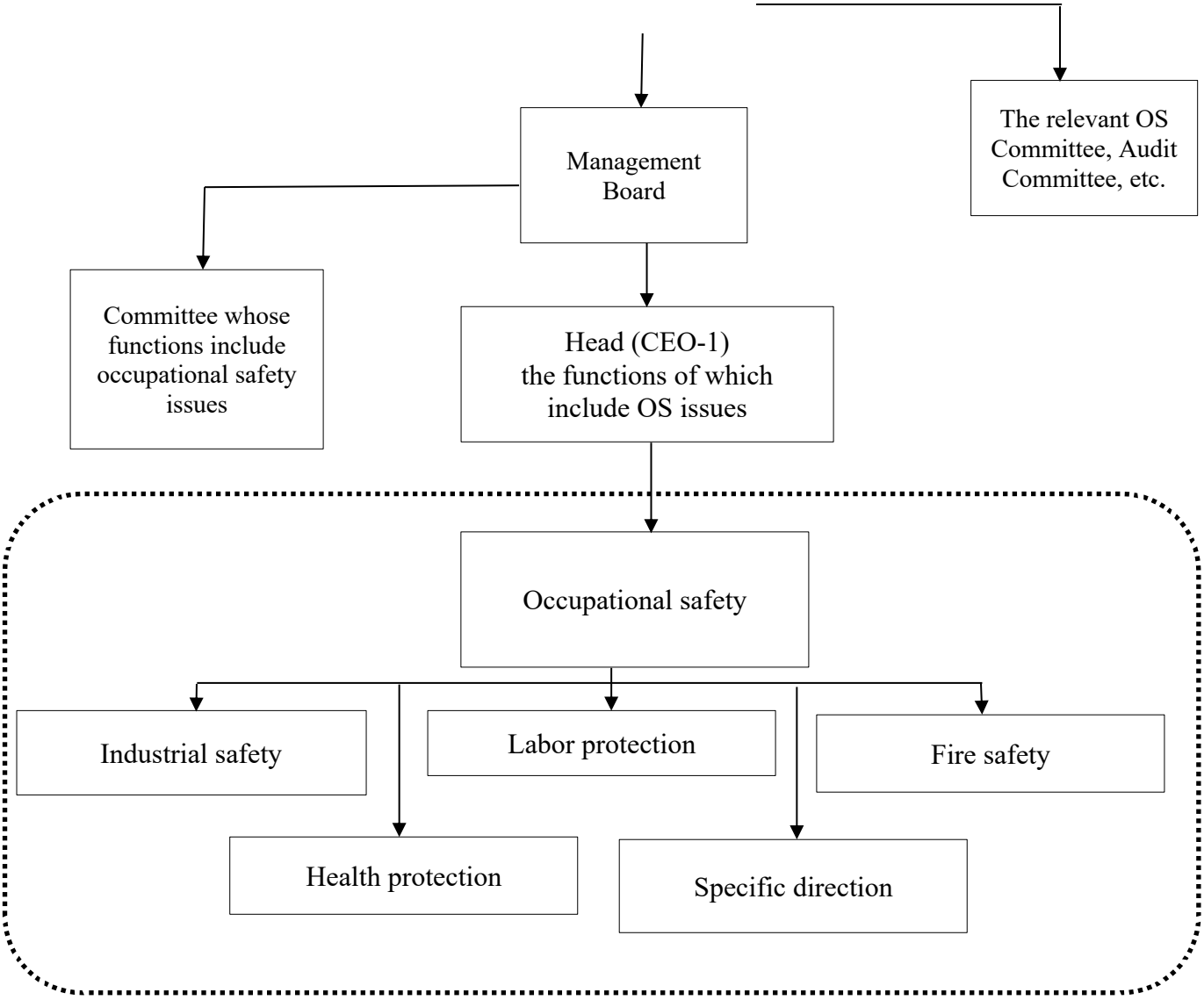
153. Upon completion of the audit, the Health and Safety Sector of the Fund sends an official letter to the Corporate Center of the PC with the audit results.

Section 7. Roles and Authorities

154. The organizational structure of the company's OS function is based on the scale of the PC itself and its structure.

155. The recommended pattern of role allocation for building the organizational structure of a OS subdivision is given below.

Standard Roles and Sample of the Organizational Structure, Interaction Procedure



Annex No.1
to the Corporate Standard on
Occupational Safety
Management for the Samruk-
Kazyna Fund Group

Recommended Methods for Determining the Root Causes

Root Causes Determining Theory.

• Accidents and incidents are unplanned events that can lead to serious consequences, such as injuries, fatalities, loss of production, property damage, and environmental disasters. Understanding the causes of these events is critical to preventing them, since without this approach it is impossible to effectively develop measures to prevent or minimize their consequences. Root cause analysis theory helps organizations not only eliminate current problems, but also improve processes, increase efficiency and quality of work, and prevent similar problems in the future.

The main types of causes that may exist in accidents:

1. Human factor

• Errors: Unintentional or accidental mistakes made by people, such as misinterpreting instructions or performing incorrect actions.

• Inattentiveness: Problems related to insufficient concentration, fatigue, information overload.

• Inadequate training and preparedness: Lack of knowledge or skills to perform the job.

• Communication failures: Errors in the transmission or perception of information among individuals.

2. Technical reasons

• Equipment failures: Breakdowns or malfunctions in equipment, mechanisms, devices, or systems.

• Equipment wear or obsolescence: The need for maintenance or replacement of equipment.

• Incorrect configuration or operation: Errors in the configuration, installation, or operation of equipment.

• Software malfunctions: Failures in the control system or malfunctioning algorithms.

3. Organizational reasons

• Poor work organization: Insufficient coordination, weak process management, or lack of resources for proper operation.

• Violation of procedures and standards: Ignoring or failing to comply with safety standards, regulations, and internal rules.

• Lack of control: Insufficient monitoring and supervision of staff actions or equipment condition.

• Failure to comply with safety requirements: Insufficient attention to safety measures and risk prevention.

4. Ecological and external causes (Environment)

- Poor weather conditions: Heavy rain, snowfall, storms, frost, which may affect processes or safety.
- Environmental impact: Air pollution, water pollution, chemical exposure, or natural disasters.
- Human factors outside the organization: For example, actions of other organizations, social or political factors that affect security.

5. Financial and resource reasons

- Lack of financial resources: Inability to invest in necessary equipment, staff training, safety measures.
- Economic instability: Financial crises or budget cuts, which may lead to a reduction in safety or quality of work.
- Human resource shortage: Lack of qualified specialists or staff shortage.

6. Process and systemic reasons

- Design or planning errors: Incorrect design of processes, infrastructure, or systems, leading to instability.
- Ineffective work processes: Processes that are not optimized or are inefficient, which can lead to errors and failures.
- System integration challenges: Incompatibility between different systems or technologies used within the organization.

7. Information and communication reasons

- Information deficiency or distortion: Inability to obtain or misinterpretation of critical information.
- Problems in communication between departments: Ineffective interaction between different levels and departments of the organization.
- Errors in documentation: Deficiencies in instructions, project documentation, or reports.

8. Social and cultural reasons

- Insufficient safety culture: Safety negligence or disregard for rules on the part of employees.
- Organizational culture: The influence of corporate culture on the perception of risks, norms, and safety standards.
- Social problems within the team: Conflicts, low morale, problems with employee motivation.

Breaking down incidents into these categories helps to analyze them more systematically and identify root causes, which in turn contributes to the development of effective solutions to prevent recurrence.

Root Causes Determining Stages:

Determining the root causes of an incident is a complex and multifaceted process that involves several key stages. These stages help to structure the analysis, identify

the true causes of the incident, and develop measures to prevent recurrence. The main stages of this process are as follows:

1. Collecting and analyzing facts

- Description of the incident: The first stage involves recording all the details of the incident — when, where, and what happened, who was involved, and what the consequences were.
- Data collection: All available data related to the incident is collected: witness statements, reports, CCTV footage, equipment maintenance reports, etc.
- Initial analysis: An initial analysis of events is conducted to understand what factors may have contributed to the incident and to rule out obvious errors.

2. Identifying hidden or systemic causes

- Systemic factors assessment: Once the immediate causes have been identified, it is necessary to check whether there are any systemic deficiencies (e.g., poor process organization, employee training issues, management deficiencies).
- Verification of procedures and standards: Existing procedures, instructions, standards, and their compliance with reality are analyzed. Ineffective or outdated regulations are often the root cause of problems.

3. Identifying factors contributing to the incident

- Analysis of the environment and conditions: It is important to assess the impact of external factors such as weather conditions, emergencies, or insufficient preparation in specific conditions.
- Organizational and cultural factors: Organizational issues such as lack of resources, weak leadership, poor corporate culture, or disregard for safety are assessed.

4. Search for possible solutions and recommendations

- Developing corrective measures: Based on the root causes identified, measures are developed to prevent the incident from recurring. These may include changes to processes, improvements to procedures, employee training, and the introduction of new technologies.
- Preventing recurrence: The risks of recurrence are assessed and strategies are developed to minimize these risks. For example, updating equipment, improving staff training systems, introducing new safety standards.

5. Documenting results and developing an action plan

- Documenting the analysis: The results of the analysis and the root causes determined are recorded in reports for future use. It is important to document not only the reasons, but also the proposed measures to eliminate them.
- Developing an improvement plan: A detailed action plan is created, including steps to eliminate the identified reasons, implementation deadlines, and those responsible for implementation.

6. Monitoring and evaluating the effectiveness of decisions

- Implementation of measures and monitoring: After corrective measures have been introduced, it is important to monitor their effectiveness in real-world conditions.

- Measurement of change: Periodic measurement is conducted to ensure that accident prevention measures are effective and that accidents do not recur.

These stages help not only to eliminate the consequences of the incident, but also to improve processes, systems, and safety culture within the organization, preventing similar incidents from recurring in the future.

Making a sequence of events.

1. Information and data collection.

- Documents and records: All available materials that may be useful for tracing the chronology of events should be collected. These may include:

- event reports (official records, logs);
- video camera recordings;
- witness statements;
- work reports and documents (e.g., inspection reports, maintenance reports).

Interview participants: If possible, interview people directly involved in the incident to get their versions of events.

2. Identification of key events

- Key events: Highlight key events that are directly related to the incident. These can include human actions, equipment operations, external factors, or changes in the process.
- Important factors: Notes on external factors such as weather, changes in policy or laws, emergencies, or other important circumstances that may have affected the incident.

3. Structuring events on a timeline

- Create a timeline describing each event that led to the incident. These are how you can do it:

- Event 1 (e.g., “Proceeded to perform the task”): description of what happened at the very beginning.
- Event 2 (e.g., “Failed equipment configuration”): description of the next important step or problem that has arisen.
- Event 3 (e.g., “Poor communication between departments”): details about possible communication errors.
- Event 4 (e.g., “Equipment malfunction”): description of the breakdown or failure.
- Event 5 (e.g., “Emergency situation occurred”): how the incident or accident happened.
- Event 6 (e.g., “Actions to address the consequences”): description of measures taken after the incident.

Each event must be described with an indication of the time or period so that the chronology can be accurately traced.

4. Root cause analysis

- Identifying connections: Try to identify connections between events. Which events directly preceded the incident? Which of them contributed to its occurrence?

- Incorrect actions or omissions: Analyze where mistakes, omissions, or incorrect decisions occurred that could have changed the course of events.

5. Forming the final sequence of events

Based on the information gathered and analyzed, compile a final sequence of events that will look like a clear chronology, starting from the initial point and ending with the outcome of the incident.

Example of a sequence of events:

1) 08:00 — The employee began checking the equipment.

2) 08:15 — During the inspection, a slight deviation in the operation of the system was noticed.

3) 08:30 — The deviation was not properly documented or reported to the technical service.

4) 09:00 — The problem with the system got worse, and the equipment started malfunctioning.

5) 09:30 — The equipment failed completely and an emergency situation occurred.

6) 09:45 — Employees began to take measures to eliminate the accident.

7) 10:00 — The emergency situation was localized and the consequences minimized.

6. Process evaluation and implementation of changes

Once the sequence of events has been compiled, it can be used to:

- Identify at which stages the incident could have been avoided;

- Determine what additional measures or changes to processes could prevent similar incidents in the future.

Compiling a sequence of events helps not only to understand what happened, but also how processes and systems can be improved in the future to avoid such incidents from recurring.

Examples of security systems.

Before proceeding to identify the root causes of the incident, it is necessary to evaluate all possible protection systems that could be involved in the course of this incident. A protection system means any control system or technical means that reduce the probability of the incident itself or the severity of its consequences:

Technical means	**Control systems and procedures**
• Emergency stop/alarm systems	• Production instructions
• Fire protection systems	• Methods of safe work (work permits)

The assessment of security systems may also include the following stages:

1. Overview of all safety systems involved:

- Technical systems, such as automated monitoring devices, emergency shutdown, alarm and security systems;
- Operational measures and actions taken by employees, including training and safety instructions;
- Procedures and standards that should have been followed.

2. Verification of security system functionality:

- Did all systems work as intended? Were they activated on time?
- Were there any malfunctions or failures in the systems?
- If the systems have worked, have they provided effective protection or minimized damage?

3. Analysis of human-technology interaction:

- How quickly and correctly did employees respond to potential threats?
- Were the instructions for using the protection systems accessible and clear?

4. Identifying weaknesses in security systems:

- Are there elements in the system that could be improved or did not work properly?
- Possibility of upgrading them to increase the security level in the future.

Only after these aspects have been thoroughly assessed, it will be possible to identify the root causes of the incident, determine what led to the security breaches, and develop measures to prevent similar situations in the future.

An example of three of many techniques for determining the root causes of accidents and applying these techniques is given below:

- the Fault Tree method;
- the Five Whys method;
- the Ishikawa Diagram method (Fishbone Diagram).

	Fault Tree	Five Whys
Data collection	Structurally organized process. Mandatory requirement.	It depends on the scale of the incident. A lesser degree of structural organization. Data is collected as needed.
Formation of a group to identify the root causes	The group is formed compulsorily.	It depends on the scale of the incident. The analysis can be carried out by one person.
Compiling a sequence of events	Compulsorily	Non-compulsorily. It is compiled as required.

Identifying protection systems	Compulsorily	Non-compulsorily. It is compiled as required.
Checking for possible causes	Compulsorily	Non-compulsorily. It is carried out as required
Development of recommendations	Compulsorily	Compulsorily
Compiling of the Report	Compulsorily	Compulsorily. Summary report.
Consideration of the and submission of the Report	Compulsorily	Non-compulsorily
Categorization of root causes	Compulsorily	Compulsorily

The Fault Tree" method can be used in the investigation of any incidents, but is used for more complex cases.

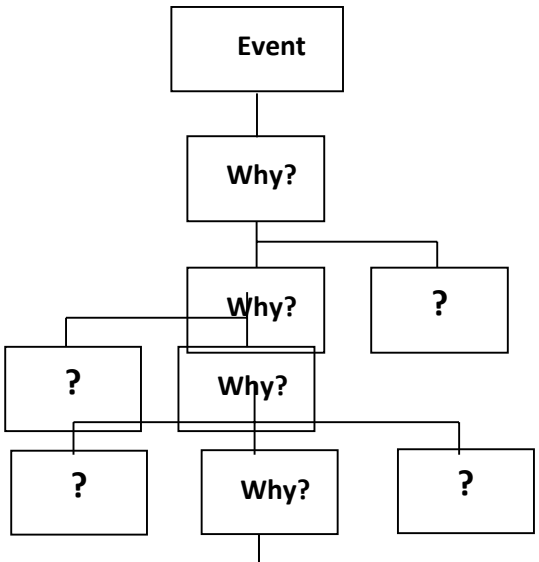
When building a "Fault Tree", use the following questions:

1) Why? Why did what is indicated in the block happen?
2) How? How did what is indicated in the block happen?
3) What logically determines what is indicated in the block?
4) What conditions must exist for what is indicated in the block to happen?
5) What else could contribute to what is indicated in the block? (Do not use conclusions of the investigation of the previous incident)
6) How can I group or classify the problems that have arisen?

The "Five Whys" method is used only for simple cases. This method is a simplified version of the "Fault Tree". It was specially designed for use by one person or a small group in the analysis of simple incidents and involves focusing attention and efforts on identifying one or two root causes, eliminating which could prevent this incident.

The analysis using the Five Whys method can be divided into the following stages:

1) identify the top-level event;
2) asking "Why?" to investigate the causes of the incident. This can be done graphically, as shown in the diagram;
3) At each level, check the result you have obtained before moving on. Do not make assumptions;
4) the root cause will most likely become apparent when answering the fifth



question “Why?”. However, finding the root cause may require more than 5 questions. Continue your analysis until you reach the systemic level cause;

5) Identify one or two root causes that could have prevented the incident;

6) If during the analysis you find out that several “branches” and several root causes are emerging, this means that the analysis should be continued using the “Fault Tree” method.

The analysis using the Fault Tree method can be divided into the following stages:

1) Specify the initial event at the top of the diagram;

2) Identify two or more actions or conditions that were the direct cause of the initial event;

3) Then, working through each “branch” of the logical tree to the end, brainstorm all the physical and behavioral reasons that could actually lead to the initial actions or conditions. At this stage, the question “Why?” arises The question that needs to be answered is formulated as follows: “Why could this happen?”;

4) Continue building this tree until you find the systemic factors of the incident;

5) After determining the first level of causes, move further down the scheme, branch by branch until the end of each branch;

6) Usually, one or more physical causes occur first, followed by one or more human causes, followed by one root cause at the systemic level;

7) When adding each next step, ask the question: “Is this the direct cause of the event or the reason indicated in the rectangle directly at the top?”

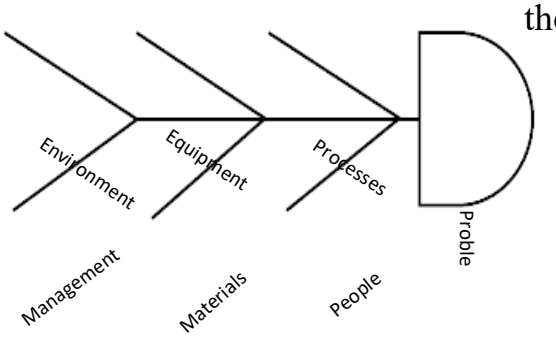
8) Each branch can end in three cases:

- the root cause has been discovered;
- a normal condition has been identified;
- a proposed cause is not a factor in the incident.

The Ishikawa Diagram (Fishbone Diagram)

Diagram structure: The diagram is shaped like a fish skeleton: the long horizontal line represents the “spine” of the fish, and the causes of the problem are displayed as “bones” extending from the central line at an angle, like that of a fish.

Diagram:



1. Identifying the problem:

The center of the diagram indicates the problem that needs to be solved. This will be the “head of the fish”.

2. Main categories of causes: To structure the causes of the problem, basic categories that may influence its occurrence are used.

There are typically 6 categories:

- **People** (human resources, personnel)
- **Processes** (work methods and processes)
- **Equipment** (machines, tools, technologies)
- **Materials** (raw materials, components, resources)
- **Environment** (working conditions, external environment)
- **Management** (management processes, strategies, and policies).

3. Subcategories of causes: Each of these categories can be supplemented with subcategories that detail specific causes. For example:

- **People:** low qualifications, poor communication, lack of motivation.
- **Processes:** unoptimized quality control process, inefficient task assignment.
- **Equipment:** machine wear and tear, frequent breakdowns.
- **Materials:** low-quality raw materials, poor storage of materials.
- **Environment:** unfavorable conditions at work, pollution of the working environment.
- **Management:** lack of strategy, inefficient distribution of resources.

Analysis and search for causes: Once the diagram has been built, it is used for systematic analysis and to identify the root causes of the problem. This helps the team to identify weaknesses in the processes and determine which factors have the greatest impact on the problem.

Example of use:

- Let’s assume that a manufacturing company has experienced a problem with product quality (the main issue is “poor product quality”). The Ishikawa Diagram will help to detail which factors from various categories (people, processes, equipment, etc.) may influence this and will enable their analysis.

The Ishikawa Diagram:

- Helps to identify all possible causes of the problem, including those that may not be obvious at first glance.

- Promotes teamwork by allowing different specialists to be involved in the analysis process.
- Improves understanding of the relationships between different aspects of the problem.
- Helps to structure information, improve the problem-solving process, and

increase efficiency in various areas.

Categorization of root causes.

One of the main advantages of conducting root cause analysis is the ability to identify recurring causes of accidents or common production problems. If we consider each incident separately, then the root causes are seen as separate problems of a one-time nature. Maintaining an incident database permits to identify trends. Categorization of causes can be carried out based on various criteria: by type of equipment, by the element of ensuring production safety, by the element of the production optimization process, by the amount of material damage, etc.:

1) risk assessment;
2) instructions and safe working methods;
3) inspections and quality control;
4) design;
5) preventive maintenance and repeated equipment failure;
6) the human factor;
7) training;
8) occupational safety in contractors;
9) transfer of information;
10) guidance, control and support;
11) investigation of accidents and potentially hazardous situations;
12) actions in emergency situations;
13) natural phenomena;
14) high-risk jobs.

The following is an explanation for each category and examples.

Category of root causes	**Explanation**	**Example of the formulation**
Risk assessment	Is the degree of risk understood correctly? Are the risk control methods used correctly? Were there any problems related to analyzing production hazards?	The methodology for determining the degree of risk is not applicable or not required.
Production instructions and safe working methods	Are there general and/or local guidelines available? Are they being used correctly? Are safe work practices used - fire work, posting locks and tags, working in confined spaces?	There is no procedure for work on hanging locks and labels. Instructions do not meet the requirements.
Design	Has the project documentation been verified? Does everything comply with norms and standards?	Project verification is not required.

	Was the “human factor” taken into account when designing?	The project does not take into account the “human factor”.
Inspections and quality control	Are the necessary inspections required and carried out? Are the right materials being used? Are they being used correctly? Is there an inspection schedule and is it being implemented?	Unsuitable materials are used – there is no system of defining compliance of materials.
Preventive maintenance and repeated equipment failures	Has the recommended maintenance work been performed or based on the compiled programs, or based on experience of previous malfunctions?	There is no program of preventive maintenance work.
Human factor	This includes confusion, fatigue, abuse and all other causes of human misconduct not related to poor performance of other systems, such as inadequate training and work planning, as well as, improper handling of equipment.	There is no distinction between types of alarm systems because the “human factor” was not considered in the design (this can also be categorized as a “Design” or “Training”).
Training	Is there a lack of training that has in any way affected this incident?	The employee has not completed the training course, there is no a system of timely completion of mandatory training courses.
Occupational safety in contractors	Is there a process in place to ensure that the contractors involved comply with the company’s requirements?	The company does not control the maintenance of HSE documentation from the contractor.
Transfer of information	Have all requirements of the instructions been brought to the attention of employees and understood by them? Have the recommendations been brought to the attention of employees? Are there any facts to support this? Are turnaround records used as a way to convey important information? Are there systems in place to ensure that information is translated correctly?	There is no requirement for compilation of turnaround records. Requirements of the instruction are incomprehensible. There is no a process of controlling knowledge of instructions.

Guidance, control and support	Is management able to provide a far-reaching vision of the situation? Does management hold staff accountable for their actions? Are there any management checks? Does management support teamwork?	Insufficient work planning. The head was not aware of what was happening.
Investigation of incidents and potentially hazardous situations	Could recommendations made as a result of an investigation of a previous accident or potential hazardous situation have prevented another accident? Did the failure to investigate the previous accident exacerbate the consequences of the next accident?	There are no requirements for investigation of potentially hazardous situations.
Staff actions in emergency situations	Did the emergency response have any effect on the scale of the incident? Could the accident have been brought under control or eliminated more quickly with more effective emergency response?	There is no system that provides training of fire service personnel to extinguish hydrocarbon fires.
Natural phenomena	This category includes natural force majeure circumstances: floods, earthquakes, hurricanes, tornadoes, and etc.	
High-risk work (earthworks, fire works, WAH, gas hazardous work, etc.)?	Has a permit document been received? Has the briefing been completed in full before starting work? Have all the preparatory measures been completed? Are the means of individual and collective protection provided for the performance of work?	Lack of control and clear requirements. Lack of personal and collective protective equipment.

Development of measures to eliminate the root causes.

The investigation team should develop recommendations or an action plan to eliminate all root causes and hazardous conditions identified during the investigation. When making recommendations, follow the proposed procedure:

Make a list of all root causes identified during the process and categorize them; Identify the most important reasons that had a big impact on this incident. If these causes are eliminated, the probability of a repeat of such incidents in the future will be

significantly reduced or completely eliminated. Availability of 5-10 root causes is normal for complex cases. 2 or 3 of these causes could have the strongest impact on the probability of an accident.

Develop an action plan to prevent a recurrence of the incident in the future. For example, if the cause of the incident was structural defects that may be present on other parts of similar equipment, then the action plan will include a stage for identifying similar problems and implementing appropriate precautions.

Make recommendations according to the list of root causes. Some measures can eliminate several causes at once. Therefore, it is always recommended to consider the root causes in a complex.

• The recommendation should be clear and understandable. In English, this concept can be expressed by the word "SMART", which in our case can be represented as an abbreviation, each letter of which means a word that carries a certain meaning:

• **S**pecific – specificity - does the recommendation specifically say what needs to be done? If you were personally given such a recommendation, would you understand what they want from you?

• **M**easurable – the ability to track the implementation – are there any quantitative indicators to find out if the recommendation will be implemented?

• **A**ccountable – personal responsibility – does the recommendation specify the person responsible for its implementation within the prescribed period?

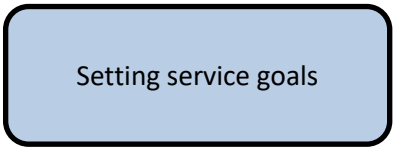
• **R**elevant – quality – will a corrective measure be able to prevent or significantly reduce the probability of a repeat incident? How realistic is implementation of this measure in general, what is its economic profitability in terms of costs, what are the technical and practical possibilities for its implementation? What problems will arise as a result of its implementation? Has the recommendation been independently reviewed by a third party (i.e., not part of the group) to identify unintended negative consequences that it may cause to the work of production and staff?

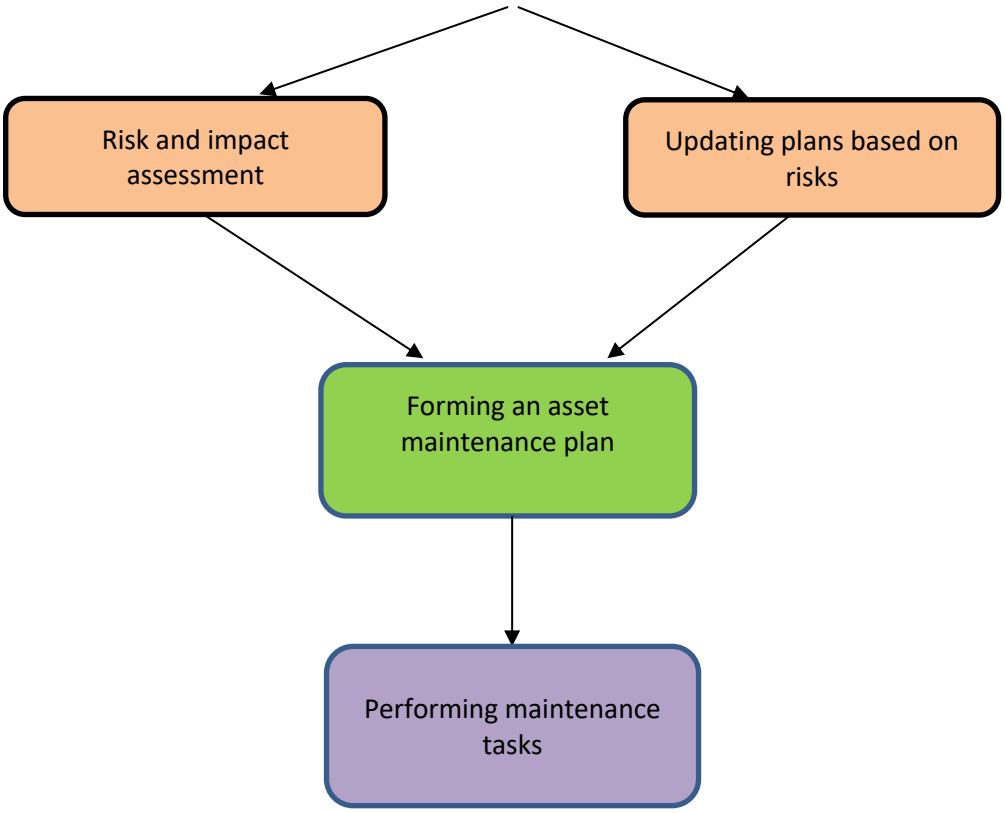
• **T**ime Limits – is the deadline for implementation of the recommendation within reasonable limits?

Annex No.2

Management System for Lean Equipment Maintenance is a process aimed at improving equipment availability at minimal cost, based on risk and impact assessment to determine priority tasks and achieve optimal business results through effective maintenance planning.

The stages of the equipment maintenance management process are presented below in the form of a flowchart.




Risk and impact assessment
Updating plans based on risks
Forming an asset maintenance plan
Performing maintenance tasks

Annex No.3

OCCUPATIONAL SAFETY AUDIT REPORT

Name of the audit object	
Type of audit	Selective audit of Samruk-Kazyna JSC
Mailing list	
Audit deadlines	

1. SUMMARY

Audit objectives	
Audit period	
Basic assumption	
Facts limiting the activities of the Commission within the scope of this audit	

The audit report is drawn up in two copies, signed by the members of the commission and representatives of the audit object.
In case of disagreement with the audit results, the representative of the audit object attaches a "dissenting opinion" to the audit report and makes a corresponding record in the audit report. Disagreement with the audit results is to be justified.

1.1 Brief information about the company

2. FINDINGS

No.	Non-compliance/Observation	Item LSI/IRD
General		
1.		
2.		
3.		
4.		
5.		

No.	Non-compliance/Observation	Item LSI/IRD
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		
31.		

Annex No.4
to the Corporate Standard on
Occupational Safety
Management for the Samruk-
Kazyna Fund Group

Procedure for Remuneration of Portfolio Companies with an Annual Nomination of the Chief Executive Officer of Samruk-Kazyna JSC for Achieving Results in the Field of Occupational Safety

General Provisions

1. The main goals of the annual nomination of the Chief Executive Officer of Samruk-Kazyna JSC for achieving high OS results include:

- improving the level of safety culture at the enterprises of the Fund group of companies;
- reducing the level of occupational injuries;
- non-material remuneration of the PC for the OS results;
- increasing the interest of all employees in the high-quality and effective performance of OS tasks;
- increasing the interest of employees of the OS services of portfolio companies in the final results of work in the field of OS.

2. The assignment of the annual nomination of the Chief Executive Officer of Samruk-Kazyna JSC in the form of the first place for achieving OS results is carried out annually on the basis of data for the reporting calendar year.

3. The procedure provides for incentives for achieving OS results for the reporting calendar year.

4. The assignment of the nomination of the Chief Executive Officer of the Fund for achieving OS results is based on uniform established evaluation criteria on the following issues:

1) the safety, preservation of life and health of employees in the course of their work;
2) development and implementation of OS standards based on the best international practices;
3) use of various proactive OS tools, monitoring, leading indicators;
4) OS performance (lagging indicators).

Procedure

5. The Occupational Health and Safety Sector of the Fund is responsible for organizing and conducting the nomination procedure.

Summing up and determining the nominated PCs is carried out by the Occupational Health and Safety Sector of the Fund on the basis of uniform established evaluation criteria in accordance with the data provided by the PCs for the reporting calendar year, which should be sent to the Occupational Health and Safety Sector of SamrukKazyna JSC no later than 15 days after the end of the reporting calendar year (Table No. 1). Employees of the Occupational Health and Safety Sector of Samruk-Kazyna JSC have the right to selectively request documents confirming the data.

6. The nomination of the Chief Executive Officer of Samruk-Kazyna JSC for achieving OS results is presented during the final annual OS meeting of Samruk-Kazyna JSC or during the annual OS Forum.

Awarding and Encouragement of Winners

7. The following type of award is established for a portfolio company that has achieved the best OS results:

The first place is a Certificate of Honor from the Chief Executive Officer of Samruk–Kazyna JSC, a plaque for the first place.

Table No.1

Evaluation criteria

Evaluation criteria	**Grades**
Availability of IRDs, digital solutions based on the best world practice:	
Occupational Safety Policy	*+1*
Life-Saving Rules	*+1*
Incidents Notification and Investigation Procedure	*+1*
Transport Safety Management Standard	*+1*
Risk Management and Assessment Standard	*+1*
Contractors Management Standard	*+1*
Fire Safety Standard	*+1*
Occupational Safety Management System Guidance	*+1*
The procedure for recording behavioral safety observations, potentially hazardous incidents, hazardous conditions, hazardous actions	*+1*
Document regulating the right to stop work (stop cards) in case of unsafe conditions or work	*+1*

Regulated program of motivation (encouragement/stimulation) of safe behavior of employees	*+1*
Goals, tasks and target indicators for achieving the set goals for occupational safety (KPI)	*+1*
** In the case of other operating IRDs in the portfolio company, the list is subject to addition (specify)*	
Availability of an effective automated system for occupational safety	*+1*
Availability of a mobile application for occupational safety	*+1*
** In the case of other digital solutions for occupational safety, the list is subject to addition (specify).*	
Availability of a valid Vision Zero concept certificate	*+1*
Availability of a valid ISO 45001 certificate in the PC corporate center	
available *not available*	*+1* *+0*
% coverage of subsidiaries by internal field audits/inspections by employees of corporate centers of portfolio companies	
10 - 20%	*+0*
21 - 45%	*+1*
46 - 70%	*+2*
≥ 71%	*+3*
Ratio of the number of eliminated inconsistencies to the number identified as part of inspections of the corporate center of the portfolio company (the deadline for eliminating which came to December 31 of the calendar	

year)	
0-30%	*+0*
31%-60%	*+1*
61%-80%	*+2*
81%-90%	*+3*
91%-100%	*+4*
Ratio of the number of eliminated inconsistencies to the number identified as part of inspections of the authorized state bodies in all areas of occupational safety (the deadline for eliminating which was December 31 of the calendar year)	
0-30%	*+0*
31%-60%	*+1*
61%-80%	*+2*
81%-90%	*+3*
91%-100%	*+4*
Increase in the number of registered SBA/SBS/SBD in accordance with the Strategy for the Development of the Occupational Health and Safety Management System of Samruk-Kazyna JSC for 2024-2028	
decrease in quantity compared to the indicator for the previous year	*0*
increase by 0-5%	*+1*
increase by 6-9%	*+3*
an increase by 10% or more compared to the previous year	*+5*
Increase in the number of identified hazardous conditions/hazardous actions and potentially hazardous incidents in accordance with the Strategy for the Development of the Occupational Health and Safety Management System	

of Samruk-Kazyna JSC for 2024-2028	
decrease in quantity compared to the indicator for the previous year	*0*
increase by 0-5%	*+1*
increase by 6-9%	*+3*
increase by 10% or more compared to the previous year	*+5*
Increase in the number of registered stop cards in accordance with the Strategy for the Development of the Occupational Health and Safety Management System of Samruk-Kazyna JSC for 2024-2028	
decrease in quantity compared to the indicator for the previous year	*0*
increase by 0-5%	*+1*
increase by 6-9%	*+3*
increase by 10% or more compared to the previous year	*+5*
% of production personnel trained in the course "Safe Work Culture"	
0-10%	*+1*
11-30%	*+2*
31-60%	*+3*
61-90%	*+4*
>90%	*+5*
% of managers and technical personnel of contractors trained in the "Safe Work Culture" course and outsourced employees performing work for a period of at least 1 year	
0-10%	*+1*
11-30%	*+2*
31-60%	*+3*
61-90%	*+4*

>90%	*+5*
% of CEO-1 level managers and employees of production structural subdivisions and occupational health and safety services who completed training and received a certificate for the IOSH course	
0-10%	*+1*
11-30%	*+2*
31-60%	*+3*
61-90%	*+4*
>90%	*+5*
% of CEO-1 level managers and employees of production structural subdivisions and occupational health and safety services who completed training and received a certificate for the NEBOSH course	
0-10%	*+1*
11-30%	*+2*
31-60%	*+3*
61-90%	*+4*
>90%	*+5*
% of drivers who completed the defensive driving course to the total number of PC drivers	
0-10%	*+1*
11-30%	*+2*
31-60%	*+3*
61-90%	*+4*
>90%	*+5*
% of drivers from contractors who completed defensive driving training to the total number of drivers providing transportation services to Subsidiaries/Branches	

of PCs	
0-10%	*+1*
11-30%	*+2*
31-60%	*+3*
61-90%	*+4*
>90%	*+5*
Number of OS meetings held by the CEOs of PC corporate centers, documented in minutes	
0	*+0*
1-2	*+1*
3-4	*+2*
>5	*+3*
Number of OS meetings held by the CEO-1 of PC corporate centers, documented in minutes	
1-5	*+0*
6-10	*+1*
11-15	*+2*
>15	*+3*
% of implementation of the annual Occupational Safety Action Plan of Samruk-Kazyna JSC	
<60%	*+0*
60-70%	*+1*
71-95%	*+2*
96-100%	*+3*
% of Technical Re-equipment Plan implementation	
<60%	*+0*
60-70%	*+1*
71-95%	*+2*
96-100%	*+3*
Fatality Accident Rate - FAR compared to last year's indicator	*Exclusion from the list of PC nominees with the presence of work-related fatalities*
Lost Time Injury Frequency (LTIF)	

in accordance with the target set in the Strategy for the Development of the Occupational Health and Safety Management System of Samruk-Kazyna JSC for 2024-2028	
coefficient = 0	*+10*
coefficient <target indicator of the Strategy by 20-30%	*+7*
coefficient <target indicator of the Strategy by 11-19%	*+5*
coefficient <target indicator of the Strategy by 6-10%	*+3*
coefficient <target indicator of the Strategy by 1-5%	*+2*
coefficient = target indicator of the Strategy	*+1*
coefficient exceeds the target indicator of the Strategy	*0*
Non-work related fatality rate - NWRF compared to last year's indicator	
coefficient = 0	*+10*
coefficient <target indicator of the Strategy by 20-30%	*+7*
coefficient <target indicator of the Strategy by 11-19%	*+5*
coefficient <target indicator of the Strategy by 6-10%	*+3*
coefficient <target indicator of the Strategy by 1-5%	*+2*
coefficient = target indicator of the Strategy	*+1*
coefficient exceeds the target indicator of the Strategy	*0*
Motor Vehicle Crash Rate - MVCR compared to the last year's indicator due to the fault of drivers of the Fund group	

organizations with injured employees	
coefficient = 0	*+10*
coefficient <target indicator of the Strategy by 20-30%	*+8*
coefficient <target indicator of the Strategy by 11-19%	*+6*
coefficient <target indicator of the Strategy by 6-10%	*+4*
coefficient <target indicator of the Strategy by 1-5%	*+3*
coefficient = target indicator of the Strategy	*+2*
coefficient exceeds the target indicator of the Strategy	*0*
Decrease in the number of accidents involving contractors' employees at production facilities compared to the last year's indicator	
at level 0	*+5*
decrease by more than 30%	*+4*
decrease by more than 20%	*+3*
decrease by11-20%	*+2*
decrease by 6-10%	*+1*
increase by 0-5%	*+0*
increase by more than 5%	*-10*
Decrease in the number of fires compared to the last year's indicator	
at level 0	*+5*
decrease by more than 30%	*+4*
decrease by more than 20%	*+3*
decrease by11-20%	*+2*
decrease by 6-10%	*+1*
increase by 0-5%	*+0*
increase by more than 5%	*-10*
Increase in the number of practical training sessions	
increase by 0%	*+0*

increase by 1-5%	*+1*
increase by 6-10%	*+2*
increase by 11-15%	*+3*
increase by more than 15%	*+4*
% of employees familiar with the circumstances of severe accidents and fatalities that occurred in the PC, of all employees of the Fund group through the distribution of information bulletins	
<60%	*+0*
60-70%	*+1*
71-95%	*+2*
96-100%	*+3*
Increase in the number of proposals for improving the OS Management System	
increase by 0%	*+0*
increase by 1-5%	*+1*
increase by 6-10%	*+2*
increase by 11-15%	*+3*
increase by more than 15%	*+4*

Annex No. 5
to the Corporate Standard on
Occupational Safety Management
for the Samruk-Kazyna Fund Group

Procedure for assigning the rating “The Most Involved CEO in Occupational Safety Issues among Samruk-Kazyna JSC Portfolio Companies”

General Provisions

1. The main goals of compiling the rating of “The Most Involved CEO in Occupational Safety Issues among Samruk-Kazyna JSC Portfolio Companies” are as follows:

- enhancing the leadership, commitment, and involvement of senior executives of portfolio companies in Occupational Safety (OS) issues;
- setting a personal example for employees in order to reduce the level of occupational injuries at the enterprises of portfolio companies and increase the interest of all employees in the high-quality and effective performance of tasks in the field of OS;
- non-material remuneration of the CEO of PC for being awarded the rating of “The Most Involved CEO in Occupational Safety Issues among Samruk-Kazyna JSC Portfolio Companies”.

2. The assignment of the rating of the “The Most Involved CEO in Occupational Safety Issues among Samruk-Kazyna JSC Portfolio Companies” in the form of the first place is carried out annually on the basis of data for the reporting calendar year.

3. The procedure provides for incentives for being awarded the rating of “The Most Involved CEO in Occupational Safety Issues among Samruk-Kazyna JSC Portfolio Companies” for the reporting calendar year.

4. The rating of “The Most Involved CEO in Occupational Safety Issues among Samruk-Kazyna JSC Portfolio Companies” in the field of occupational safety is assigned based on the unified established assessment criteria for the following issues:

1) taking personal responsibility for ensuring safety and protecting the life and health of employees during labor activities;

2) applying a proactive approach to occupational safety management;

3) personal participation in improving the occupational safety management system.

Procedure

5. The Occupational Health and Safety Sector of the Fund is responsible for organizing and conducting the assigning procedure.

Summing up and determining the nominated PCs is carried out by the Occupational Health and Safety Sector of the Fund on the basis of uniform established evaluation criteria in accordance with the data provided by the PCs for the reporting calendar year, which should be sent to the Occupational Health and Safety Sector of

Samruk-Kazyna JSC no later than 15 days after the end of the reporting calendar year (Table No. 1). Employees of the Occupational Health and Safety Sector of Samruk-Kazyna JSC have the right to selectively request documents confirming the data.

6. The awarding of the winner of the rating "The Most Involved CEO in Occupational Safety Issues among Samruk-Kazyna JSC Portfolio Companies" takes place during the final annual OS meeting of Samruk-Kazyna JSC or during the annual OS Forum.

Awarding and Encouragement of Winners

7. The following type of award is established for the winner:

A Certificate of Honor from the Chief Executive Officer of Samruk–Kazyna JSC, a plaque for the first place.

Table No.1

Evaluation criteria

Evaluation criteria	**Grades**
Personal obligations in the field of occupational safety signed and undertaken by the Chief Executive Officer	
available	*+1*
not available	*0*
% of personal obligations fulfilled in the field of occupational safety	
0-30%	*+0*
31%-60%	*+1*
61%-80%	*+2*
81%-90%	*+3*
91%-100%	*+4*
Number of OS meetings held personally by the Chief Executive Officer with PC enterprises, documented in minutes	
0	*+0*
1-2	*+1*
3-4	*+2*
>5	*+3*
Availability of a video or written address from the Chief Executive Officer to employees	

regarding the need to comply with occupational safety requirements	
there are both video and written addresses	*+3*
video address	*+2*
written address	*+1*
not available	*0*
Number of personally conducted by the Chief Executive Officer of SBA/SBS/SBD, safety cards	
0	*+0*
1-2	*+1*
3-4	*+2*
>5	*+3*
Availability of a comprehensive corporate KPI for occupational safety	
available	*+5*
not available	*0*
Availability of a training certificate for the course "Safe Work Culture"	
available	*+3*
not available	*0*
Availability of a training certificate for the IOSH course	
available	*+3*
not available	*0*
Availability of a training certificate for the NEBOSH course	
available	*+3*
not available	*0*
Facts of visits by the Chief Executive Officer to Subsidiaries and branches, and conducting occupational safety audits with the preparation of Reports	
0	*+0*
1	*+2*
2-3	*+3*
>5	*+5*

Absence of fatalities	*+5*
Absence of accidents with severe outcome	*+3*
Visit by the Chief Executive Officer to the scene of an accident, fire, or other incident, with the preparation of meeting minutes	*+3*