Translation

APPROVED:
by the Board of Directors
of Public Joint Stock Company “Severstal” on 17 October 2019
(MINUTES № 9/2019 dated 17 October 2019)

Risk Management and Internal Control Policy of Public Joint Stock Company “Severstal” and Related Legal Entities

1 GENERAL TERMS

1.1. The Risk Management and Internal Control Policy ("the Policy") of Public Joint Stock Company "Severstal" (PAO Severstal, "the Company") and related legal entities (hereinafter collectively referred to as "the Company") has been developed subject to the Federal Law "On Joint Stock Companies", the Tax Code of the Russian Federation and other Russian statutes, the Charter and internal documents of PAO Severstal as well as recommendations of the Corporate Governance Code approved by the Board of Directors of the Bank of Russia on March 21, 2014 and recommendations of international professional organisations related to risk management and internal control, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

1.2. This Policy defines a concept, goals and focuses of the Risk Management and Internal Control System of the Company as well as responsibilities and authorities of the Company's Board of Directors and its executive bodies necessary to ensure their functioning.

1.3. This Policy covers PAO Severstal and its related legal entities which statements are used to prepare PAO Severstal's consolidated financial statements in line with International Financial Reporting Standards (IFRS).

2. FORMATION OF THE RISK MANAGEMENT AND INTERNAL CONTROL SYSTEM

2.1. Goals of the Risk Management and Internal Control System

An effective Risk Management and Internal Control System ("the System") has been developed and is applied to ensure reasonable confidence in achievement of the Company's goals:

- strategic goals to create and maintain the Company's value;
- operational goals related to results of the Company's financial and economic activities and soundness of its assets;
- goals ensuring that the Company's activities are in compliance with applicable laws and internal policies, regulations and procedures, occupational, industrial, environmental safety as well as information and personal security;
- goals ensuring that reliable accounting (financial) statements or non-financial internal and/or external reporting are prepared appropriately and in due time.

An effective functioning of the System should ensure that there is proper control over the Company's financial and economic activities.

2.2. Tasks of the System

The System has been established to:

- identify, analyse and assess risks arisen at all organisational levels of the Company, manage such risks effectively, including effective allocation and use of available risk management resources;
- improve the Company's risk management and internal control processes;
- create a reliable information basis to plan activities and take well-considered management decisions;
- develop internal control procedures to ensure effective application of the Company's business processes;
- standardise and regulate key risk management and internal control procedures;

- set up an optimal organisational structure in the Company in line with its requirements and based on the segregation of duties principle (between and within the entities of the System);
- ensure soundness of the Company's assets and effective application of the Company's resources;
- ensure integrity, transparency and reliability of the Company's financial and non-financial statements for internal and external use, and other information to be disclosed, subject to applicable laws and regulations;
- ensure effective application of control procedures to mitigate risks of involving the Company in corrupt and fraudulent practices;
- check counterparties and analyse their anti-corruption procedures, prevent and eliminate conflicts of interests;
- ensure that the Company complies with applicable law and internal policies, regulations and procedures.

2.3. Key definitions

Internal control means a process performed by the Board of Directors, executive bodies and all employees of the Company to ensure reasonable confidence in achievement of the Company's goals related to its operating activities, preparation of financial statements and reporting and law compliance. Internal control is an integral part of the risk management system, while risk management is a continuous and cyclic process in the whole Company management system.

Risk means probability of events which may have a negative impact on achievement of the Company's goals.

Risk appetite means the amount of risk in qualitative or quantitative terms which the Company is ready to take while implementing its strategy and achieving its goals.

Risk management means culture, opportunities and practices integrated with the strategy process and performance which the Company relies on as part of risk management while creating, maintaining and realising its value.

2.4. System constraints

The Company assumes that certain System constraints are possible which may affect the achievement of the Company's goals due to the following factors:

- subjective judgments by System participants when selecting internal control procedures, including in terms of cost assessment and benefits after their implementation;
- lack of resources to implement the System tasks;
- external events out of the Company's control;
- errors made by System participants because of their negligence or having insufficient competency;
- deliberate violations of the established policies and procedures by the Company's employees for illegal purposes to make personal profit or improve the presentation of the Company's performance.

3. SYSTEM COMPONENTS

The System of the Company is a combination of related components which structure complies with the established methodology COSO ERM and COSO IC-IF[1].
The System consists of the following related components:

- control environment;
- strategy and goal setting;
- risk identification and assessment;
- risk response;
- control procedures;
- information and communications;
- monitoring.

3.1. **Control environment** means the culture and atmosphere within the Company created by its Board of Directors and executive bodies which is a basis for all other System components and ensures an effective structure and appropriate actions.
The control environment involves:

- the system of values, code of conduct and business ethics;
- commitment to the Company's values and ethical principles demonstrated by the Company's management;
- supervision over the System implementation and application by the Company's Board of Directors;
- the organisational structure with delegated powers and responsibilities.

3.2. **Strategy determination and goal setting** in the Company are continuously integrated with risk identification and assessment:

- the Company's strategy is determined based on external and internal business environment;
- the risk appetite depends on the Company activities and is in line with its strategy;
- the Company analyses alternative strategies and assesses risks and opportunities of all of them;
- business goals are set following the Company's strategy and are a framework to identify, assess and respond to risks.

3.3. **Risk identification and assessment** means a process of identifying and assessing events which may have a negative impact on:

- achievement of the Company's goals;
- reliability of accounting (financial) statements and non-financial internal and/or external reporting;
- soundness of assets;
- compliance with laws and the Company's internal policies, regulations and procedures.

Risks are identified at different management levels in the Company. The Company's executive bodies ensure that risks are regularly identified as part of the System. Key risk reports are submitted to the Company's Board of Directors for review twice a year.

[1] COSO ERM Enterprise Risk Management – Integrating with Strategy and Performance, COSO IC-IF Internal Control – Integrated Framework are methodological risk management and internal control documents. COSO means the Committee of Sponsoring Organizations of the Treadway Commission.

3.4. **Risk response**

The Company prioritises risks to identify an appropriate risk response strategy and allocate risk management resources.

The risk response strategy is chosen following the business environment, benefit/cost ratio, risk appetite and risk significance.

A possible risk response practice is to mitigate it by implementing control procedures.

3.5. **Control procedure** means a risk mitigation activity. They may include a wide range of activities such as approving, granting permissions for, checking, verifying, analysing reports on current activities, limiting physical access and separating powers.

Control procedures are implemented **at three business process levels** (operations) in the Company:

- before the business process (operation) starts to prevent and minimise a negative impact of events and factors which may effect on achievement of the Company's goals;
- when implementing a business process (operation) to identify on a timely basis and immediately eliminate, violations and deviations from set parameters arising in the process;
- after the business process (operation) has been finalised to ensure reported data is true and assess whether results comply with target (planned) parameters.

Control procedures are divided into preventative and identifying **by types**.

- ***Preventative control procedures*** prevent something incorrect or wrong happening due to automatic blocking or additional checking

- ***Identifying control procedures*** identify errors already made

Control procedures are divided into manual, IT dependent and automated **by implementation**.

Manual control procedures:

- are implemented beyond information systems;
- are done by the Company's employees only manually;
- may be both preventative and identifying but error prevention is rarely effective.

IT dependent control procedures:

- are implemented by standard or non-standard information system algorithms;
- require participation of the Company's employees;
- are divided into systematic (e.g. delivery order approval) and reporting (report analysis);
- may be both preventative and identifying.

Automated control procedures:

- are implemented by standard or non-standard information system algorithms;
- are done without intervention from any Company employee;
- are mainly preventative, i.e. prevent something incorrect or wrong happening.

Control procedures shall be described in the Company's internal documents and reported to its employees.

3.6. **Information and communications** play a key role in the System. The effective working of the System depends on complete and true information on the Company's activities being available and provided in due time as well as a reliable system which generates, transfers and processes such information and communicates decisions taken. It involves:

- efficient collection of complete and true information on risks, including information collected via hot lines;
- correct processing of information to take the best decisions, including by using state-of-the-art technologies;
- communications within the Company on possible and implemented events and the System-related decisions taken;
- timely transfer of information on risks to the Audit Committee, the Board of Directors and executive bodies of the Company;
- periodic reporting on risk identification and management by the Company's functional divisions to executive bodies, the Audit Committee and the Board of Directors;
- disclosure of information on key risks and internal control in the Company's annual report.

3.7. **Monitoring** means regular assessment of the System performance in order to:

- analyse in the System opportunities to achieve the appropriate targets;
- assess whether the Company can adequately respond to changes in its activity and the environment;
- identify significant shortfalls of the System;
- develop measures to improve the System.

System monitoring is done at different management levels and involves:

- continuous supervision of control and follow-up of risk management activities and their performance by the Company's executive bodies and employees within their competences;
- regular self-assessment of the System performance by executive bodies;
- System performance assessment by the Company's Internal Audit Department and reporting identified shortfalls to the divisions;
- review of the System performance analysis and assessment results by the Company's Audit Committee and Board of Directors.

System assessment results are used to prepare a section in the Company's annual report.

4. RESPONSIBILITY FOR THE SYSTEM ORGANISATION AND APPLICATION

A reliable basis for risk management and internal control is fundamental to ensure proper corporate management. Various participants play key roles in the Company to ensure a reliable basis for risk management and internal control.

4.1. Board of Directors

The Company's Board of Directors defines the principles of and approaches to the organisation of the System in the Company.

The Company's Board of Directors is required to do the following in terms of the System:

- determines the Company's strategy;

- develops and implements the System based on which the Company's executive bodies may manage key risks;
- characterises and determines the risk appetite of the Company in order to achieve its strategic goals (risk appetite);
- forms an appropriate culture and system of remuneration in the Company;
- approves the main risk management practices;
- monitors and analyses risk management and internal control systems;
- monitors the outcome of the self-assessment made by executive bodies of the System's performance and recommends actions to improve the System (if necessary);
- ensures reliable internal and external information and communication processes, bears responsibility for external communications on risk management and internal control.

4.2. **Executive bodies**

The Company's executive bodies develop and maintain an effective risk management and internal control system in the Company and implement decisions taken by the Board of Directors and related to the organisation of the System.

The Company's executive bodies are required to do the following in terms of the System:
- implement and execute the System principles, policies and procedures approved by the Company's Board of Directors on a daily basis;
- assign responsibilities and authorities required to ensure the System's application and ensure an appropriate reporting structure;
- include functions and responsibilities related to risk management and control procedures into job descriptions for the Company's employees and develop System-related KPIs;
- identify and manage risks within their competences on a regular basis;
- develop and implement control procedures;
- monitor control procedure performance (self-assessment) and develop improving activities on a regular basis;
- inform the Company's Audit Committee and the Board of Directors on their assessment of the condition of the System on a timely basis.

4.3. **Risk Management and Internal Control Department**

In order to ensure and maintain System performance, the Company has a separate division - Risk Management and Internal Control Department and is a part of AO Severstal Management – PAO Severstal's management company.

The main tasks of the Risk Management and Internal Control Department are to:
- coordinate System development and application processes;
- develop, implement and update corporate standards regulating the risk management and internal control process;
- arrange training courses related to risk management and internal control for the Company's employees;
- analyse a portfolio of risks and make suggestions on how to respond to them and allocate resources related to appropriate risk management;
- coordinate periodic reporting on the risk management performance and on other issues covered by this Policy for the Audit Committee, the Board of Directors of the Company and executive bodies of the Company;
- prepare consolidated statements on risks;

- ensure day-to-day control of how the Company's divisions and related legal entities manage risks;
- implement advanced risk management and internal control practices.

4.4. Internal Audit Department

The Company's Internal Audit Department provides to the Audit Committee and executive bodies reasonable and objective assurance that an efficient risk management, internal control and corporate governance system has been developed and is applied in the Company.

The Internal Audit Department's functions in terms of the System are regulated by the Regulations for Internal Audit of the Company.

5. COOPERATION WITH EXTERNAL PARTIES INVOLVED, STATE REGULATORY AUTHORITIES, EXTERNAL AUDITORS, BANKS, INSURANCE COMPANIES, SHAREHOLDERS, INVESTORS AND OTHER PARTIES CONCERNED

The Company's divisions involved in risk management and internal control, as part of their activities, cooperate with external parties concerned, state regulatory authorities, external auditors, banks, insurance companies, shareholders, investors and other parties subject to the law and appropriate local statutes of the Company and on issues within their competence.

6. CLOSING PROVISIONS

6.1. This Policy as well as any amendments or supplements hereto shall be approved by the Board of Directors of the Company.

6.2. Should any individual clause of the Policy be in conflict with the applicable law or the Company's Charter as a result of change thereto, the Policy shall be applicable to the extent to which it does not conflict with the applicable law and the Company's Charter.