



Public Joint-Stock Company  
NOVOLIPETSK STEEL

**APPROVED BY**

the Board of Directors  
of Novolipetsk Steel

Minutes No. 276  
“22” December 2020

**INTERNAL CONTROL  
AND RISK MANAGEMENT POLICY**  
of Novolipetsk Steel

(Original Enactment)

Lipetsk  
2020

## Contents

<b>1.</b>	<b>GENERAL PROVISIONS .....</b>	<b>3</b>
<b>2.</b>	<b>TERMS AND DEFINITIONS.....</b>	<b>3</b>
<b>3.</b>	<b>GOALS AND OBJECTIVES OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM .....</b>	<b>3</b>
<b>4.</b>	<b>WORKING PRINCIPLES OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM .....</b>	<b>4</b>
<b>5.</b>	<b>COMPONENTS OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM .</b>	<b>5</b>
	5.1. Management and culture. ....	5
	5.2. Strategy and goal setting.....	6
	5.3. Functioning.....	6
	5.4. Control procedures .....	8
<b>6.</b>	<b>DISTRIBUTION OF RESPONSIBILITY AND AUTHORITY OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM .....</b>	<b>9</b>
	6.1. Level I: Board of Directors/Audit Committee.....	9
	6.2. Level II: Management Board, Risk Management Committee, Investment Committee (regarding investment project risks). ....	9
	6.3. Level III: RM FA and compliance system. ....	10
	6.4. Level IV: Risk owners. ....	10
<b>7.</b>	<b>INDEPENDENT PERFORMANCE ASSESSMENT OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM .....</b>	<b>10</b>
<b>8.</b>	<b>PROCEDURE FOR APPROVING AND REVISING THIS POLICY.....</b>	<b>11</b>

## 1. GENERAL PROVISIONS

This Internal Control and Risk Management Policy of Novolipetsk Steel (hereinafter the Policy) sets out the goals, objectives, working principles, and assignment of powers and responsibilities of the Internal Control and Risk Management System (hereinafter ICRMS), and the procedure for independent evaluation of ICRMS effectiveness.

This Policy has been developed in accordance with the current legislation of the Russian Federation, the Corporate Governance Code recommended by the Central Bank of the Russian Federation, the Charter of Novolipetsk Steel (hereinafter the Company), the Anti-Corruption Policy, and recommendations by international professional organizations dealing with risk management and internal control, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

## 2. TERMS AND DEFINITIONS

2.1. The following terms are used in this document with the corresponding definitions:

- 2.1.1. **Risk owner:** any employee who is responsible for the management, monitoring and control of an identified risk, including the implementation of the selected responses. Risk owners are assigned top-down for all process levels: from strategic to local business processes.
- 2.1.2. **Acceptable risk level (risk appetite):** the acceptable level of losses that the Company could sustain in the process of attaining its goals.
- 2.1.3. **Investment Committee:** a collective body established for the development, preparation, and adoption of resolutions related to investment activities.
- 2.1.4. **Risk Management Committee:** a collective body established to ensure the effectiveness of risk management and the internal control system, as well as to promote business ethics and anti-corruption principles.
- 2.1.5. **Risks:** any potential events, circumstances, internal or external factors impacting goal attainment.
- 2.1.6. **Risk radar:** a report about the level of critical and substantial risks, the current and approved standard levels of key risk indicators (hereinafter KRI), the implementation status and cost-effectiveness of management measures, and the materialized risks and their consequences.
- 2.1.7. **ICRMS:** a set of administrative measures, methods, procedures, corporate culture norms, and actions taken by the Company to attain the optimal balance between risks and increasing the value of the Company's assets.
- 2.1.8. **Compliance system:** a system ensuring the compliance of the Company and its employees with Russian, international, and applicable foreign legislation, internal standards, and the Company's organizational and administrative documents.
- 2.1.9. **Risk level:** the combination of a risk's probability and the consequences of its materialization, expressed in a certain formalized manner.
- 2.1.10. **RM FA:** Risk Management functional area.

## 3. GOALS AND OBJECTIVES OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM

The ICRMS is an integral part of corporate governance. Its creation is aimed at ensuring reasonable confidence in the attainment of the Company's strategic and operational goals.

The functioning of the ICRMS is systemic and integrated into strategic and operational management at all levels. It applies to all units and all Company employees in the exercise of their functions.

The key goals of the Company's ICRMS are as follows:

- Ensuring sufficient confidence in the attainment of the Company's goals.
- Ensuring the efficiency of financial and business activities and cost-effective resource use.

The key objectives of the Company's ICRMS are as follows:

- Timely detection and management of risks impacting the Company's goal attainment.
- The Company's timely adaptation to changes in the internal and external environment.
- Safeguarding Company assets.
- Meaningfulness and sustainability of project activity results.
- Integrity and reliability of accounting (financial), statistical, management, and other reporting.
- Control over compliance with legislation, as well as the Company's internal policies, regulations, and procedures.

#### **4. WORKING PRINCIPLES OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM**

**Leadership.** The Company's management ensures the dissemination of internal control and risk management knowledge at all management levels, promotes the formation of an effective system for communicating detected risks, and encourages the development of a risk-based corporate culture.

Assignment of decision-making levels. The level of risk management decision-making is determined depending on how critical the risk is and its impact on the attainment of Company goals.

**Continuity and comprehensiveness.** The ICRMS functions on a continuous basis, covering all areas of Company activity and all types of risks emerging in the course of operation.

**Value creation and protection.** The ICRMS is aimed at attaining goals and enhancing activities in employee health and safety, compliance with legislation and other normative requirements, environmental protection, quality of processes and projects, operation efficiency, and reinforcing the Company's business reputation.

**Integration into decision-making processes.** The ICRMS is an integral part of the Company's corporate governance system, aimed at increasing decision-making process efficiency in key areas of activity, such as strategic planning, the budget process, investment, and operational activities.

**Systemic and structural nature.** The Company is committed to a systemic approach to establishing the ICRMS which enables the consideration of the system as a whole, taking into account any interrelations between its elements, and an assessment of decision efficiency.

Risk-based approach. The intensity (form, scope, complexity, duration, frequency) of risk management and control measures is determined based on how critical each risk or area is for the Company.

**Adaptivity and priority.** The approaches adopted as part of the ICRMS are in line with the internal and external situation (context) and the risk profile. The first priority is to adopt the risk management and control measures necessary to address the most critical risks.

**Assignment of powers and responsibilities.** In order to reduce the risk of an operational error or fraud, powers and responsibilities are divided between various ICRMS members so that one unit

or employee would not have both the responsibility to fulfil a function and the power to control its fulfilment.

**Use of best available information.** When making risk-based assessments, analysing, and making decisions, managers rely on the following information sources, in order of priority: historical data, experience, feedback from subject area experts and stakeholders, observations, forecasts, expert assessments.

**Transparency.** The ICRMS ensures the timely and full-scale involvement of all stakeholders, including decision-makers, and guarantees that their opinion is duly noted when determining the risk profile.

**Rationality and adequacy.** The Risk Management System considers the cost-effectiveness of risk management measures. Risks are reduced based on the scale of the impact risks have on deviations from target indicators and the amount of resources required for to reduce them. The scope and complexity of risk management measures and control procedures must be necessary and sufficient for risk reduction.

**Responsibility.** All ICRMS members are responsible for the identification, analysis, evaluation, minimization, and monitoring of risks in the course of their activities, as well as the development and implementation of measures for risk management and control tools.

**Formalization.** The ICRMS permits reasonable procedure formalization with content taking precedence over form.

**Human and cultural factors.** The ICRMS takes into account personal and cultural differences in perception and motivation that could prevent the Company from attaining its goals.

**Resources.** The Company provides the sufficient resources for risk management purposes.

**Effective information sharing.** The Company builds up a robust mechanism for sharing information and reporting to ensure maximum risk management effectiveness.

## 5. COMPONENTS OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM

The Company's ICRMS consists of interrelated components (5.1–5.4), each being a necessary tool for goal attainment and acting as part of a common set of measures.

- 5.1. **Management and culture:** a set of local regulations, rules, formal and informal procedures, common opinions and attitudes characterizing the functioning of the Company's ICRMS, reflecting its values, impact on corporate culture and mode of activity.

The main factors determining this ICRMS component are as follows:

- The Board of Directors carrying out its risk management supervisory function. The Board of Directors/Audit Committee assesses ICRMS efficiency through its contribution to value creation.
- The divisional process-based Company management model. The Company sets up the organizational structure, reporting line, powers, and responsibility areas for internal control and risk management. The structure is determined based on the Company's strategic goals.
- Defining the target culture. The Company has created a risk culture that determines its approach to risk identification, analysis, and management. The risk-based approach used in decision-making is part of the corporate culture.
- Motivation. The Company motivates its employees to adopt the risk-based approach by including risk-related indicators into the KPI system.
- Demonstrating commitment to key values. Understanding the Company's key values lays the foundation for the ICRMS. The key corporate values and principles are stipulated in the Corporate Ethics Code.

- Training in ICRMS principles. Training programmes for Company employees implemented as part of risk culture development and of the compliance system support the effective functioning of the Company's ICRMS at the risk owners' level.
- Recruitment, development, and retention of qualified specialists. The Company pursues a strategy of constant employee development and upskilling, adheres to its policy of hiring, encouragement, and non-financial incentives, and reconsiders its requirements to employees to reflect any changes in the Company's goals.

**5.2. Strategy and goal setting:** preconditions for risk detection and evaluation.

The Company determines its strategic goals and subsequently cascades them down to FA and division goals and objectives. The ICRMS goals and objectives are in accordance with the Company's strategic focus areas.

The main factors characterizing strategic planning and goal setting from the ICRMS perspective are:

- Analysis of business conditions. The Company takes into account both internal and external business conditions when developing its strategy, which is also reflected in the ICRMS goals and objectives.
- Risk appetite assessment. The Company assesses its risk appetite. The approaches to risk appetite assessment take into account the characteristic aspects of the Company's activities.
- Assessment of strategic alternatives. The Company analyses alternative options for strategy implementation, including via a risk and opportunity analysis.
- Formulation of business goals. The Company's tolerance to losses determines the acceptable degree of deviation from its goals. Therefore, such tolerance is an attribute of the goals, not of particular risks.

**5.3. Functioning** is a continuous cyclical process made up of the following stages:

- Risk identification. The Company has created a system for detecting the risks to which the Company is exposed and categorizing them by source and type.

The Company uses four risk identification systems: (1) declaration system: risks are identified based on threats detected by owners or any Company employees; (2) if data sets are available, RM FA employees identify risks by analysing these sources; (3) RM FA employees analyse external open-source information; (4) RM FA employees analyse the results of planned checks, audits, and diagnostic tests to detect any breaches and risks.

- Risk impact assessment. The ultimate goal of risk assessment is forecasting potential losses/damage to the Company and determining the risk criticality level.

Risk assessment draws both on qualitative (conditional scales with experts assigning importance) and quantitative methods (based on publicly available or Company-collected statistics, or on expert assessments in case statistics are lacking/not applicable).

Risk evaluation methodologies are developed jointly by RM FA specialists and business unit specialists.

The risk evaluation system is in a constant state of development aimed at improving measurement accuracy. The accuracy and adequacy of the applied methods is analysed annually (the values of risk factors predicted by the model are compared to real changes).

The aggregate risk assessment for several types of risks is made taking into account the correlation of risk factors.

For management purposes, all risks, depending on their assessment, are broken down into critical, substantial and low risks. Low risks are the ones manifested in individual local

processes, substantial ones – in end-to-end processes, and critical ones have an impact on the goals of the entire Company.

The company prioritizes risks to determine an adequate risk response strategy and to allocate resources to manage them. The risk criticality criteria are determined by the Risk Management Committee.

- Management. Risk management is a set of plans and measures aimed at reducing undesirable consequences and the probability of losses within the approved risk appetite;

Risk appetite is a set of KRI limits that are approved on an annual basis by the Board of Directors/Audit Committee and characterize the maximum risk threshold that the Company intends to accept, covering all key aspects of the Company's activities.

Based on the ratio of the current and planned risk level, one or another risk management strategy can be adopted, taking into account the cost of its implementation: (1) eliminating the source of the risk; (2) accepting the risk in full (in cases where the probability is extremely low or the potential damage does not exceed the cost of risk reduction); (3) accepting the risk to a limited extent (using the system of limits, collateral, hedging, insurance); (4) avoiding the risk (in cases where there is no obvious effective way to reduce the risk and its consequences are unacceptable to the Company).

Measures to manage critical and substantial risks are approved by the Board of Directors/Audit Committee; similarly, risk management measures can be approved by a collective executive body as part of regular activities, that is, by the Management Board, the Risk Management Committee and the Investment Committee. Approved measures are fixed in the minutes of meetings of collective bodies with the appointment of a person responsible for implementing these measures and meeting the deadlines. The Company exercises control over the implementation of the collective bodies' resolutions.

- Monitoring and control. The Company's regular monitoring and control of the risk level allows for analysing the effectiveness of management measures, identifying new threats, and determining the main problem areas requiring a response.

The Company monitors all changes in its current activities and in the external environment, and assesses their impact on achieving strategic goals and the risk profile.

The Company analyses risks and performance based on the following criteria: attainment of the Company's goals, the level of deviation from the set goals, materialized risks that affected goal attainment, compliance of the accepted risk level with the set goals, and accuracy of risk assessment.

The Company constantly assesses the potential for improving ICRMS efficiency, draws up and implements an ICRMS improvement plan.

- Risk reporting, information, and communication. The Company's risk reporting meets the requirements of completeness, reliability, regularity, consistency, and timeliness.

The ICRMS is based on modern information technologies that improve the quality and efficiency of decision-making. Increased attention is paid to modern data analysis technologies (Data Science) enabling the analysis of large quantities of data thus facilitating more informed and well-considered decisions.

The Company's employees are aware of the risks, goals, and tasks they face when performing internal control and risk management functions within their competence. The Company has established a system for information disclosure and communication with customers, suppliers, regulators, shareholders, and investors.

The risk reporting prepared by the RM FA is the main method to communicate information

about risks to stakeholders. Information about the risk level is reported at several levels: routine reporting at the level of risk owners, reporting to the Risk Management Committee, reporting to the Management Board and the Board of Directors/Audit Committee. ICRMS reporting at the Board of Directors/Audit Committee level is linked to the Company's strategy, business goals, and performance. The frequency and completeness of reporting is determined by the management based on the activity profile and business needs.

5.4. **Control procedures.** The Company has an internal control system (hereinafter ICS) in place, which ensures that necessary actions are taken against risks that may impede the achievement of the Company's goals, including:

- Entity Level Controls (ELC) are ICS measures which are taken by the Company's management to create a control environment and impact risk coverage in several processes at once. The ELCs are structured taking into account international practice and applicable standards. They define business ethics and rules for conducting financial and economic activities.
- Process controls are ICS measures taken by the Company's management and employees to cover process risks, including algorithms and locks implemented in IT systems; organizational and system (logical) division of power in processes; reconciliation of data in documents; expert reviews, tests, laboratory studies, visual inspections; collective (commission) decision-making; manual or automated monitoring of process parameters; procedures of analysing management data for decision-making.
- IT General Controls (ITGC) are ICS measures aimed at ensuring the integrity and differentiation of access to data, and the stable operation of the Company's information systems. The ITGCs are necessary for ensuring the reliability of process controls implemented using information systems.

The Company seeks to improve the ICS by:

- Analysing basic processes and determining the volume and types of key transactions in the chain of basic processes, risks, and control procedures aimed at covering them.
- Checking (testing) the effectiveness of control procedures through a mass or selective analysis of actual data on deviations in the basic processes and the implementation of control procedures for the relevant period.
- Assessing the materiality of the identified shortcomings in the ICS, developing and coordinating measures to strengthen it.

When developing the ICS, the Company is guided by the following principles:

- When developing measures to strengthen the ICS, priority is given to group preventive automated controls that prevent deviations in basic processes at an early stage while minimizing the human factor.
- The absence of regulatory documents governing the implementation of control procedures is not a significant drawback in itself, just as their presence does not ensure the effectiveness of control procedures. At the same time, regulatory activity is one of the most efficient ways to implement control procedures and/or ensure their proper implementation.
- For control procedures which detect deviations, it is mandatory to indicate and implement in practice effective corrective measures taken by the performer of control procedures when deviations are found.

The Company applies a risk-based approach when planning the development of the ICS in processes, based on the results of procedures for identifying and assessing risks.



## **6. DISTRIBUTION OF RESPONSIBILITY AND AUTHORITY OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM**

Internal control and risk management is a hierarchal process, which corresponds to the Company's organizational structure.

### **6.1. Level I: Board of Directors/Audit Committee.**

- Defines the principles and approaches to the organization of risk management, internal control, and internal audit in the Company.
- Approves the Internal Control and Risk Management Policy.
- Reviews and approves the Company's strategy taking into account the Company's risks.
- Approves and reviews risk appetite.
- Considers and monitors the most substantial risks to which the Company is exposed.
- Monitors the reliability and effectiveness of the ICRMS, including carrying out performance assessments of the Company's risk management and internal control procedures, as well as preparing proposals for their improvement.
- Provides continuous supervision over the functioning of the Company's ICS.
- Exercises control over procedures ensuring the Company's compliance with legal requirements, as well as ethical norms, the Company's rules and procedures, and stock exchange requirements.
- Analyses and assesses the execution of the conflict of interest management policy.
- Exercises control over countermeasures against bad faith acts of employees and third parties.

### **6.2. Level II: Management Board, Risk Management Committee, Investment Committee (regarding investment project risks).**

The Management Board, guided by the principles and approaches to the organization of the ICRMS defined by the Board of Directors/Audit Committee, ensures that the System is created and functions effectively, and, within its remit, makes decisions on individual aspects of ICRMS organization.

The Risk Management Committee, set up to strengthen the ICRMS and anti-corruption measures:

- Approves the principles, strategy, and documents regulating the risk management and ICS processes.
- Regularly reviews the Risk Radar.
- Approves and carries out general supervision over the implementation of risk management measures.
- Regularly reviews the results of analysis and assessment of ICRMS reliability and efficiency in the context of business processes, corporate and general IT procedures.
- Coordinates the work of units involved in the risk management and ICS process.
- Manages the compliance with the Code of Corporate Ethics and the Anti-Corruption Policy.
- Regularly reviews reports on compliance with business ethics and anti-corruption principles in the Company.

The Investment Committee (regarding investment project risks):

- Exercises general control over risk magnitude, selection, inclusion in the budget, and execution of risk management measures for investment projects.

### 6.3. **Level III: RM FA and compliance system.**

For the effective functioning of the ICRMS, a special structural unit was set up. The specialists of the Internal Control and Risk Management unit:

- Shape the general risk management concept.
- Develop methodological and regulatory documents on risk management.
- Foster the risk-based corporate culture.
- Assess and regularly monitor the level of accepted risks, assess the efficiency of risk management measures.
- Put forward proposals for the development of risk management action plans and risk reduction measures.
- Prepare risk reports.
- Regularly and systematically assess the reliability of the ICS at the Company's ELC level, process level, and ITGC level and implement corrective measures together with operating units.

The Company also has a compliance system in place, the functions of which are distributed among several specialized structural units.

### 6.4. **Level IV: Risk owners.**

Risk owners:

- Regularly identify risks and threats.
- Communicate risks and threats to the RM FA.
- Monitor set KRIs.
- Keep risk levels within the approved limits.
- Implement the risk management action plan.

## 7. **INDEPENDENT PERFORMANCE ASSESSMENT OF THE INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM**

The independent performance assessment of the ICRMS is carried out by the Company's Internal Audit Department, which operates on the basis of a risk-based Audit Plan approved by the Audit Committee after it has been previously reviewed by the Chair of the Audit Committee and the CEO (Chairman of the Management Board) of the Company. The ICRMS performance assessment includes:

- Analysing compliance of business process goals with the Company's goals.
- Identifying flaws of the ICS which precluded (are precluding) the Company from attaining its goals.
- Verifying the reliability and integrity of business processes and information systems, including procedures for countering illegal and bad faith actions, abuse, and corruption.
- Verifying the efficiency of control procedures and other risk management measures, including the efficient use of resources allocated for such purposes.
- Assessing the performance of measures aimed at eliminating violations and flaws of the ICS and improving it.
- Verifying the reliability of accounting (financial), statistical, management, and other reporting.
- Verifying the efficiency and appropriateness of resource use.
- Verifying asset protection.
- Verifying compliance with Russian legislation and internal documents.

- Ensuring the adequacy and maturity of risk management system elements.
- Verifying whether all risks have been identified and if the Company's management assesses risks correctly across all management levels.
- Analysing information on the materialized risks.

## **8. PROCEDURE FOR APPROVING AND REVISING THIS POLICY**

This Policy and all additions and amendments to it are subject to approval by the Company's Board of Directors.

In the event that any change in laws and regulations of the Russian Federation results in certain clauses of this Policy coming into conflict with them, such clauses shall become void, and the Company shall abide by the current legislation of the Russian Federation until this Policy is revised accordingly.

The requirements of this Policy apply to all business units of the Company.