

RISK MANAGEMENT

A VIGILANT APPROACH

In 2022, Metinvest reviewed its risk management practices to address the significant changes that the Group has undergone. The vigilant approach underpinning the risk management methodology proved itself in the reporting period.

MANAGING RISKS RELATED TO WAR

In response to the challenges that arose as the full-scale war started, Metinvest adhered to robust risk management strategies aimed at responding to first-tier risks (outside management's control) and mitigating second-tier risks (related to the normal course of business).

Confronted by the Russian Aggression, Metinvest faced the necessity to assess new risks by addressing the following concerns:

- preserving the safety and well-being of those working within territories affected by hostilities
- organising and providing humanitarian aid to the local communities
- determining the optimal use of production capacities
- adapting the logistics model
- ensuring steady utility supplies
- overseeing financial flows

While the fundamentals underpinning the risk management approach were unchanged, the primary objectives for 2022 centred on utilising available production capacities and securing access to sales markets, particularly given the logistical constraints that emerged. Throughout these challenges, the Group remained committed to a risk-oriented, decision-making approach at all levels of management.

RISK MANAGEMENT PRACTICE

Metinvest's fundamental risk management principles are defined in its Internal Audit Policy, which integrates the strategic guidance of the ISO 31000:2018 Risk Management standard. The internal regulations covering dedicated functions also include risk management aspects specific to their business processes, which helps the executive team to guide their decisions using the risk-based approach in place.

Metinvest applies an internal categorisation of risks as commercial or non-commercial. Commercial risks include, but not limited to, those that can be quantified and are directly associated with product and financial flows from operations, as well as with investments in tangible and intangible assets. Non-commercial risks are not directly associated with product and financial flows from operations, or with investments in tangible and intangible assets and include sustainability risks.

The Group delineates the primary roles and responsibilities for risk management. The Economics and Business System Development Directorate is responsible for assessment and monitoring commercial risks. The Internal Audit Directorate is entrusted with overseeing of non-commercial risks.

Metinvest identifies and measures principal risks that directly affect its operational activities and financial outcomes, incorporates these risks into its business planning processes, and develops strategies to mitigate their impact.

As part of these comprehensive risk mitigation efforts, the Group continued to assess commercial risks by analysing the

sensitivity of expected or planned EBITDA to various risk factors. This approach enabled it to adapt and respond to the evolving risks associated with the war.

To mitigate non-commercial risks effectively, management applies a corporate framework to assess the probability and impact of such risks.

RISK MANAGEMENT STRUCTURE

GRI 2-12



SUSTAINABILITY RISK MANAGEMENT

The continuous monitoring of sustainability risks is a prerequisite for ensuring the effectiveness of the Group's approach to sustainable development. The table on this page describes the factors leading to each risk's occurrence, along with the mitigation measures undertaken.

KEY SUSTAINABILITY RISKS AND MITIGATION EFFORTS IN 2022

RISK AND ITS DESCRIPTION	MEASURES TO MINIMISE RISKS
Workplace safety	
<ul style="list-style-type: none"> Workplace injuries and fatalities 	<ul style="list-style-type: none"> Safe Workspace programme Projects related to certain critical risk factors under safety roadmap Health and safety training and incentive tools for employees Safety assessment of contractors involved in hazardous works
Environmental issues	
<ul style="list-style-type: none"> Environmental impacts, including air pollution, wastewater discharges and waste generation 	<ul style="list-style-type: none"> Measures to exclude and reduce impact due to the shelling of assets Monitoring compliance with regulatory requirements Initiatives to improve energy efficiency Trust Line to raise environmental concerns Implementing technical measures to reduce the environmental impact Application of the precautionary principle when planning investment projects
Climate change	
<ul style="list-style-type: none"> Impact on business sustainability Legislative requirements to accelerate low-carbon transition 	<ul style="list-style-type: none"> Best practice approach to the calculation and disclosure on direct and indirect GHG emissions Analysis of climate-related corporate governance and risk management system Analysis and preparation for the CBAM test regime
Business ethics and compliance	
<ul style="list-style-type: none"> Fraud and corruption 	<ul style="list-style-type: none"> Adherence to the Code of Ethics and Code of Business Partnership Trust Line and incident investigation Mandatory verification of suppliers and customers for anti-corruption element Internal security screenings for all senior and high-risk positions
Counterparty sanctions risks	
<ul style="list-style-type: none"> Regulatory penalties and operational disruptions due to non-compliance Reputational damage 	<ul style="list-style-type: none"> Monitoring legislative changes in key jurisdictions Compliance function approval for new counterparties Verifying and blocking transactions with sanctioned/high-risk counterparties
Information security	
<ul style="list-style-type: none"> Losses due to critical information leaks Critical equipment or process interruption due to information system failure 	<ul style="list-style-type: none"> Organisational and technical actions to identify, categorise, protect and monitor the security of confidential information and personal data Analysis of IT infrastructure security Measures for safe remote work Training and testing IT user skills to prevent phishing attacks