Remuneration of executive bodies

In line with Nornickel's Articles of Association, the remuneration and reimbursement payable to members of the Management Board are determined by the Board of Directors..

KPI system

Remuneration of the Company's senior management, including individuals who are members of the Management Board, is comprised of basic salary and bonuses (variable part). Bonuses comprising the variable part of senior management's remuneration are based on a KPI system aligned with Nornickel's strategic goals, depend on the Company's performance, and are linked to both financial (EBITDA and FCF; weight: 40%) and non-financial metrics (work-related injury rate (weight: 10%), zero environmental incidents (weight: 10%)) as well as other individual KPIs. KPIs are updated on an annual basis by the Corporate Governance, Nomination, and Remuneration Committee of the Board of Directors. In 2024, health, safety, and environment (HSE) KPIs had a significant weight (20%) in senior management's KPI scorecards, which confirms that safety culture remains top of mind for Nornickel.

Determining the remuneration and bonuses payable to the Company's President falls within the remit of the Board of Directors.

Remuneration of Board members and the President

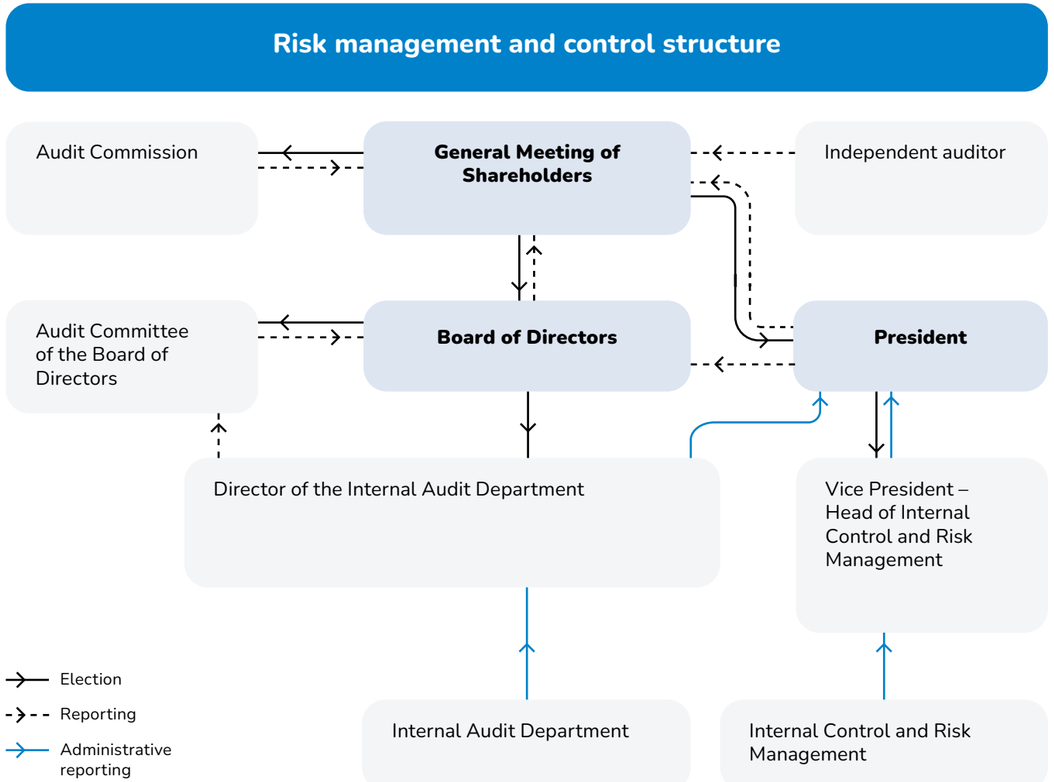
Type of remuneration	2024	
	RUB mln	USD mln
For serving on the Management Board	2.6	0.03
Salary	3,563.9	38.5
Bonuses	1,325.7	14.3
Reimbursement	0.2	0.003
Other	–	–
Total	**4,892.4**	**52.8**

Control bodies

The Company has in place a risk management and internal control system (RMICS) covering all business processes and all management levels across the Group. The control system, integrated into the Company's corporate governance processes, is geared towards achieving goals related to accurate financial reporting, operational efficiency, and compliance.

The system comprises the following control bodies:

- Audit Commission
- Audit Committee of the Board of Directors
- Internal Audit Department
- Internal control system
- Risk Management Service
- Independent audit (external control)



Audit Commission

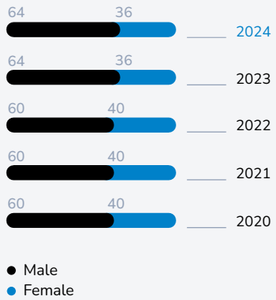
The Audit Commission serves as the control body that monitors the financial and business operations of the Company. The five members of the Audit Commission are elected annually at the Annual General Meeting of Shareholders.

In 2024, the Audit Commission audited Nornickel's business operations for 2023, with the auditors' report presented to the shareholders as part of materials for the Annual General Meeting of Shareholders. Results of the audit of the Company's business operations for 2024 will be reported to the Annual General Meeting in 2025.

Remuneration

The Annual General Meeting of Shareholders set total remuneration at RUB 1.8 million per year for each member of Nornickel's Audit Commission who is not an employee of the Company. The above remuneration level is similar to the remuneration rate set for 2023. Members who are Nornickel employees are not paid remuneration for their service on the Audit Commission. No bonuses or other rewards were paid in 2024.

Members of the Audit Commission by gender (%)



Audit Commission's remuneration

Type of remuneration	2022		2023		2024	
	RUB mln	USD thousand	RUB mln	USD thousand	RUB mln	USD thousand
For serving on the Audit Commission	7.2	105	7.2	84	7.2	78

Internal audit

The Company's internal audit function is carried out by the Internal Audit Department, established to support the Board of Directors and executive bodies in enhancing the efficiency of business process management and evaluating the risk management and internal control system. The Department operates in accordance with the Regulations on the Internal Audit Department. The Company maintains an Internal Audit Policy, approved by the Board of Directors.

The Internal Audit Department regularly conducts objective and independent audits, which include assessments of the effectiveness of the internal control system (ICS) and the corporate risk management system (CRMS). Based on the results of these audits, the Department prepares reports for senior management with recommendations for improving internal controls and monitors the development of remedial action plans, if any violations are identified.

Results for 2024

In 2024, the Internal Audit Department audited the following areas:

- Maintenance and repair management and operation of automated process control systems at production sites
- Investment projects
- Production-related transport services
- Corporate processes (procurement, charitable activities, monitoring roles of the Head Office)
- IT asset management

The Internal Audit Department is strongly focused on driving the adoption of digital data processing methods. Data analytics methodologies have been integrated into audit procedures since 2020. For the past two years, a continuous audit covering 100% of the Company's procurement activities has been successfully carried out. In 2025, this technology is planned to be piloted for other business processes.

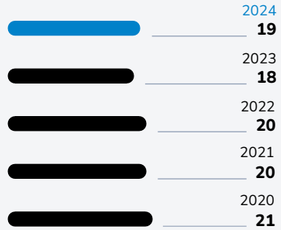
Based on recommendations issued during audits, management develops corrective actions. During 2024, over 200 initiatives were completed, aimed not only at remedying non-conformities but also at addressing the root causes of identified deficiencies.

The Internal Audit Department continuously monitors the implementation of actions developed by management, with analytical reports on the types and number of initiatives regularly reviewed by the Audit Committee.

The Audit Committee commended the performance of the Internal Audit Department for the reporting period.

The Internal Audit Department also conducted an annual performance evaluation of the Company's CRMS and ICS for 2024, concluding that both systems are generally effective, with only some minor areas for improvement identified. The evaluation results were reviewed by the Audit Committee and the Board of Directors.

Audits (NUMBER)



To ensure independence and objectivity, the Internal Audit Department reports functionally to the Board of Directors through the Audit Committee and administratively to Nornickel's President.

Evaluation

In accordance with the Internal Audit Standards, the Internal Audit Department undertakes an annual self-evaluation, the results of which are regularly reviewed by the Audit Committee and the Board of Directors.

The 2024 self-evaluation incorporated learnings from the implementation of the Roadmap for Internal Audit Function Development. The self-evaluation results indicate that the practices of the Internal Audit Department generally conform to applicable standards, with certain areas identified for improvement.

Plans for 2025

The audit plan addresses the Company's principal risk areas with due regard to priorities, incorporates thematic requests from the Audit Committee and executive management, and includes mandatory annual assessments of the Company's RMICS effectiveness.

The Internal Audit Department's work plan for 2025 was approved by the Board of Directors and includes 18 audits across the following areas:

- Audit of operational processes
- Audit of corporate processes
- Audit of operations of branches and subsidiaries
- IT audits
- Annual evaluations

Internal control system

Nornickel maintains a comprehensive internal control system (ICS), built in line with international (COSO) and Russian best practices. The Internal Control Department is responsible for ensuring the operation and development of the ICS, creating a strong control environment, establishing a risk assessment framework for business processes, implementing controls, and segregating duties and access rights in information systems.

The Internal Control Department uses a risk-based approach to conduct regular monitoring of the Company's business processes. The Company also continuously monitors compliance with regulatory requirements to combat the unlawful use of insider information and market manipulation, as well as money laundering, terrorist financing, and proliferation financing..

ICS performance evaluation

The Company performs an annual self-evaluation of its ICS within the scope approved by the Management Board. Self-evaluation procedures are automated and facilitated through the SAP GRC PC system. Reports containing the evaluation results are reviewed by Nornickel's management and the Audit Committee of the Board of Directors.

The self-evaluation results for the reporting year indicate that the Company's ICS generally operates effectively, with areas identified for improvement. Management addresses and mitigates internal control gaps, develops corrective actions, and monitors their implementation. In the reporting year, the ICS maturity level reached level 4 out of 5, designated as "Mature".

Corporate Trust Line speak-up programme

Reporting channels (24/7)

- 8 (800) 700-19-41, 8 (800) 700-19-45
- 1st Krasnogvardeysky Drive 15, Moscow, Russia, 123112, Corporate Trust Line of MMC Norilsk Nickel
- skd@nornik.ru
- Reporting form on the nornickel.ru website
- Nika corporate app

The Company does not retaliate against whistleblowers who raise concerns via the Corporate Trust Line, meaning that no disciplinary action or sanction is taken, including employees' demotion, forfeiture of bonuses, dismissal, etc. Any reports of retaliation against whistleblowers for using the Corporate Trust Line are thoroughly investigated, with the involvement of the Company's security teams. Whistleblower status is regularly monitored at all levels to detect any cases of undue pressure. Since 2023, the Company has also implemented a system for collecting feedback and assessing whistleblower satisfaction with the process.

Reports claiming breaches of ethical standards and principles are reviewed by a commission convened by the head of the unit responsible for conducting the requested investigation. If the reported information is confirmed, management takes steps to resolve conflict situations, once again explains the need for employees to comply with ethical business standards, and holds town-hall meetings. Employees can be disciplined over violating ethical standards and principles.

Key CTL principles

1. Keeping reports confidential
2. Keeping whistleblowers anonymous
3. Investigating all submitted reports in a timely and objective manner

To enhance the effectiveness and timeliness of measures designed to prevent ethical breaches, including corruption, discrimination, and human rights violations, Nornickel has implemented a Corporate Trust Line speak-up programme. Both Company employees and external stakeholders are encouraged to use the Company's confidential hotline to report any suspected breaches. All reports submitted to the Corporate Trust Line are handled with strict confidentiality, promptness, and impartiality, irrespective of the position held by the individual cited in the report.

CTL report statistics

Indicators	2020	2021	2022	2023	2024
Number of incoming reports	1,037	1,243	1,463	2,079	1,279
Number of accepted reports	451	422	589	859	651
Including confirmed breaches:	118	96	159	193	180
Ethical standards and principles[1]	–	–	*13*	*21*	*15*
Corruption	*0*	*0*	*0*	*0*	*0*
Human rights violation	–	–	*0*	*0*	*0*

Detailed report statistics are published annually in the Sustainability Report.

[1] Ethical Standards and Principles as well as Human Rights and Freedoms were designated as distinct topics within the classifier in 2022.

Corporate ethics and compliance

Nornickel conducts its business with honesty, transparency, and ethical integrity, maintaining a high level of corporate culture, which strengthens the Company's business reputation and helps build trusting relationships with investors, partners, employees, and other stakeholders.

Commitment to business ethics

Nornickel operates on the foundational principle of upholding an impeccable reputation and adhering to ethical business practices. The safe labour, life, and health of its employees are the Company's non-negotiable priorities. The Company maintains a Business Ethics Code, which is regularly reviewed and updated. The Code applies to all employees and is essential for ensuring compliance with professional standards and alignment with Nornickel's core values.

Nornickel's ethical principles:

- Protection of the Company's resources
- A responsible attitude towards the Company's information and reputation
- Integrity
- Fostering a culture of partnership and mutual respect
- Maintaining high ethical standards

Mechanisms are in place for any employee to report potential breaches of the Code; such reports are subject to investigation and review by relevant units. To encourage adherence to ethical principles and integrity at work, the Company has established a system of employee awards and incentives.

Throughout its history, the Company has not recorded any instances of mass strikes, layoffs, or widespread salary reductions.

To address potential breaches of the Code, procedures are in place for employees to safely and confidentially report relevant situations. All reports are subject to investigation. The Company guarantees that no disciplinary action or sanctions, including dismissal, demotion, or bonus forfeiture, will be applied to employees who report breaches of the Code.

Training is provided to employees to explain the Code, including a training module on the Code integrated into the Our Values programme, the Nornickel Live Q&A session, and Corporate Dialogues.

Insider information

Control in the area of combating unlawful use of insider information and market manipulation (CUUIIMM) is a part of the Company's ICS. The Company[1] operates robust compliance procedures and maintains ongoing monitoring of compliance with regulatory requirements in the CUUIIMM area.

The Company has developed and regularly updates internal documents regulating the processes in the CUUIIMM area:

- Regulations on Procedures for Access to Insider Information and Rules for Protection of Insider Information Confidentiality and Control over Compliance with the Requirements of Laws Related to Combating Insider Information Unlawful Use and Market Manipulation
- Internal Control Rules for Preventing, Detecting, and Stopping the Unlawful Use of Insider Information and Market Manipulation
- Regulations on the Procedure for Keeping the List of the Company's Insiders.

The List of the Company's Insider Information is posted on its official website under the To Insiders section.

To ensure internal control and mitigate regulatory risk within the CUUIIMM area, Nornickel has designated a dedicated officer responsible for enforcing the internal control rules. The officer conducts regular monitoring of the Company's compliance with legal requirements in the CUUIIMM area and submits reports to the Company's President regarding compliance status and the implementation of internal control measures.

Nornickel has developed remote learning courses on handling insider information, available to all employees of the Company. Completion of the courses, hosted on the Nornickel Academy corporate university platform, is mandatory for new hires..

AML/CFT[1] compliance

The Company implements a set of measures to prevent money laundering, terrorist financing, and the proliferation of weapons of mass destruction (AML/CFT).

AML/CFT internal controls are embedded into the Company's ICS and are run continuously by designated employees across all relevant units.

The key internal document in this area is PJSC MMC NORILSK NICKEL's Internal Control Rules on AML/CFT (the "Internal Control Rules"). The Internal Control Rules are updated in a timely manner to reflect changes in applicable legislation.

The Company has designated a dedicated officer responsible for monitoring compliance with AML/CFT legislation and mitigating related regulatory risks and the risks of potential employee involvement in money laundering schemes.

Reports on the implementation and effectiveness of the Company's Internal Control Rules are submitted to the President of Nornickel. These reports include information on the implementation of internal control programmes, the number of suspicious transactions reported to the Federal Financial Monitoring Service, and assessments of the effectiveness of the ICS and the level of AML/CFT regulatory risk.

Anti-corruption compliance

Nornickel is building a robust anti-corruption compliance system to manage corruption risks, ensure compliance with all relevant anti-corruption legal requirements, and safeguard the Company against involvement in corrupt practices.

In 2024, Nornickel once again maintained its leading position in the annual Anti-Corruption Ranking of Russian Business, achieving the highest possible rating of AAA+. This achievement highlights the consistent and effective operation of the Company's anti-corruption compliance system and its strong commitment to anti-corruption standards and the principles of transparent, honest business conduct.

Nornickel has a zero-tolerance policy towards corruption at all levels of the organisation, complies with the anti-corruption laws of the countries where it operates, and sets high standards of responsible business conduct for both employees and partners.

Nornickel's management sets the tone from the top by role-modelling zero tolerance for corruption in all its forms and manifestations across all levels while emphasising the critical importance of adhering to ethical standards in the performance of job duties..

Nornickel's anti-corruption compliance system, comprising policies, procedures, and controls, is subject to regular review and improvement. Through these efforts, the Company ensures that it upholds its corporate values, eliminates or mitigates corruption-related risks, and remains in full compliance with applicable regulatory requirements.

Anti-corruption policies and procedures are applicable across the entire Group.

For more information regarding adopted anti-corruption policies and procedures, as well as implemented anti-corruption measures and preventative programmes, please see the dedicated Anti-Corruption section of the Company's website.

Nornickel does not engage with political parties, affiliated foundations, or related organisations, nor does it provide funding for facilitation payments.

[1] The Company is subject to Federal Law No. 224-FZ dated 27 July 2010.

[1] Nornickel is subject to Federal Law No. 115-FZ, On Anti-Money Laundering and Combating the Financing of Terrorism, dated 7 August 2001.

Identification of corruption risks

A critical component of developing a robust anti-corruption compliance system is the identification, analysis, and assessment of corruption risks. The Company identifies potential instances of corruption among its employees and the specific business processes exposed to such illegal practices. Through this process, corruption risks are identified. Identified corruption risks are analysed to determine potential methods of committing corruption offenses within business processes, including identifying the roles of employees who may be involved in such practices. An assessment is conducted to determine both the likelihood of the identified corruption risk and the potential damage to the Company should this risk materialise. The Company regularly employs corruption risk management mechanisms, including control and monitoring of anti-corruption measures and procedures, and uses a wide range of tools to assess and eliminate potential corruption risks when engaging with counterparties.

Nornickel is committed to minimising corruption risks in both current and new business processes, and therefore conducts anti-corruption reviews of its internal documents to ensure that they present no potential for corruption. If such potential is identified, the document owner is advised to amend the paragraph or section in question as necessary.

Once every two years, the Company submits a declaration to the Anti-Corruption Charter of the Russian Business to prove its compliance with anti-corruption requirements.

In 2024, to further develop and improve its anti-corruption compliance system, the Company:

- assessed the effectiveness of controls implemented to mitigate corruption risks
- adapted and launched a mechanism for informing counterparties of its anti-corruption requirements and principles
- conducted an employee questionnaire survey to evaluate the state of corruption and the effectiveness of anti-corruption initiatives at the Company's branches and representative office
- launched the implementation phase for automating the conflict of interest management module
- delivered a training campaign on mitigating corruption risks in counterparty interactions for Group employees responsible for implementing anti-corruption compliance procedures
- established a framework for tracking inquiries from regulatory and supervisory authorities regarding anti-corruption compliance
- took measures to monitor and assess compliance with the legal requirements of the Russian Federation regarding the employment of and contracting with former government officials
- revised and updated its anti-corruption procedural documents.

Training

Compliance with the Company's anti-corruption principles is achieved when each employee feels a strong sense of personal ownership. When joining the Company, all employees take an induction briefing on compliance with anti-corruption laws, familiarise themselves with anti-corruption documents, and are required to sign an agreement setting out their anti-corruption responsibilities.

Nornickel also provides employees with regular training in anti-corruption, involving them in on-the-job anti-corruption programmes.

The Company delivers effective training tailored to different target audiences: for example, all employees take an annual online anti-corruption course, HR employees complete a course on anti-corruption compliance for HR services, and members of the Board of Directors and Management Board take an online course on anti-corruption for managers. All courses culminate in a test serving as the final step in the learning process. Remote learning courses are offered through the Nornickel Academy corporate university platform.

As of the end of 2024, the percentage of employees that the Company's anti-corruption policies and methods have been communicated to was 100%. During the year, approximately 11 thousand employees received training on anti-corruption legal requirements and corporate regulations.

Training and awareness statistics

Activities	2020	2021	2022	2023	2024
Employees that have received training on anti-corruption	5,721	9,805	31,025	25,800	10,507
Employees that the Company's Anti-Corruption Policy has been communicated to	73,810	76,626	81,492	81,347	78,826

Managing conflicts of interest

One of the priority areas within the anti-corruption compliance system is managing conflicts of interest, which can be a root cause of corruption. The Company's Regulations on the Prevention and Management of Conflicts of Interest require any pre-conflict situations or actual conflicts of interest to be disclosed both at the time of hiring and during employment, particularly when personal interests are involved. The Regulations further require employees to take timely action to prevent any potential conflicts of interest.

In 2024, the Company developed and published an interactive memo on conflict of interest management, available on its corporate portal. The Company set up standing conflict of interest commissions across the organisation to enhance the effectiveness of preventing, identifying, and resolving conflicts of interest, as well as to ensure legal compliance and improve corporate culture.

The Company upholds and promotes among its employees a culture of zero tolerance for corruption Various channels are available for reporting suspected cases of corruption, including anonymous options.

For more details on anti-corruption efforts, including the Company's conflict of interest management process, please see the 2024 Sustainability Report.

Nornickel will not tolerate any retaliation, disciplinary or other action against an employee who reports a concern about suspected corruption, or refuses to offer a bribe, facilitate bribery, including commercial bribery, or take part in any other corrupt practices.

All Group employees and partners have free and convenient access to information about the Company's anti-corruption policies and measures, available on its official website in the Anti-Corruption section.

The Company continuously monitors and implements measures to prevent, detect, and mitigate the risks of corporate fraud. The Company convenes round-table discussions to review requirements for work in specific areas and the implementation of dedicated controls designed to mitigate corporate fraud risks. The Company pays particular attention to the operation of information channels, including the CTL. The Countering Corporate Fraud online course was successfully integrated into the mandatory training programme for all employees.

Regular internal inspections are conducted to investigate suspected instances of corporate fraud or corruption. In 2024, the Company conducted 122 such inspections. Based on evidence of illegal actions against Company assets or interests discovered by Company employees, law enforcement authorities initiated 55 criminal cases related to corporate fraud and 5 criminal cases related to corruption.

In 2024, two reports about potential employee corruption were received via the CTL. Following the review and investigation of all submitted reports, no evidence of employee corruption was found.

Statistics on CTL reports about corruption or fraud

Indicators	2022	2023	2024
Number of CTL reports accepted for investigation, broken down by topic:			
Corruption	0	4	2
Corporate fraud	3	10	6
Number of confirmed CTL reports, broken down by topic:			
Corruption	0	0	0
Corporate fraud	0	2	4

Anti-corruption measures for counterparties

Nornickel strives to maintain respectful, strong business relations with its partners and does not prohibit giving and receiving business gifts, provided these are consistent with common business practices. The requirements and criteria regarding business gifts are set out in the Regulations on Business Gifts applicable to all Company employees.

The unbiased selection of the best proposals, Nornickel's procurement owner, customer, and secretary of the collective procurement body follow these rules:

- Procurement relies on the principle of division of roles
- Commercial proposals submitted by suppliers are compared using objective and measurable criteria approved prior to sending a relevant request for proposal
- The selection results and the winning bidder in the material procurement process are approved by the collective procurement body comprised of representatives from various functions of Nornickel
- A master agreement containing an anti-corruption clause is signed or renewed annually with each supplier. The anti-corruption clause outlines the course of action to be taken between the supplier and Nornickel with respect to risks of abuse. Moreover, by signing the master agreement, suppliers acknowledge that they have read the Company's Anti-Corruption Policy.

Red flags, including signs of price fixing, conflict of interest, lobbying for bidders, and unreasonable restrictions, were also incorporated into the procurement system.

To ensure the Company's economic security, more than 35 thousand reliability checks were conducted, covering both potential and existing counterparties. These assessments reviewed counterparties' reliability, solvency, financial stability, legal compliance, corruption risks, and ability to meet contractual obligations. Based on these checks, 252 entities received negative assessments, and 56 counterparties were added to the Company's register of unreliable counterparties. These contractors were listed due to the provision of knowingly false information, breach of contract, or evasion of contract execution following competitive bidding procedures.

Antitrust compliance

The antitrust compliance system in place at the Company since 2017 establishes the processes for the timely prevention, identification, and elimination of causes and conditions facilitating antitrust violations and ensures compliance of the Company and its corporate entities with applicable laws.

Nornickel carries out an internal assessment and identifies business units whose activities are exposed to antitrust risks. At such units, the Company designates antitrust compliance owners and briefs them on the applicable prohibitions and restrictions under antitrust laws.

Antitrust risks are identified and mitigation measures are developed based on information provided by these antitrust compliance owners as well as through legal support of the Group's business processes. These processes cover investment projects (such as establishing and operating joint ventures), tariff decision making, deregulating certain activities, establishing procedures for counterparty engagement (such as infrastructure access terms), modifying infrastructure operations (e.g. through revamps), entering new markets for the Company's products, and more.

Management decisions across the Group are made with due regard for antitrust legal requirements, and the existing antitrust compliance system continues to demonstrate its effectiveness.

Management decisions across the Group are made with due regard for antitrust legal requirements, and the existing antitrust compliance system continues to demonstrate its effectiveness. In 2024, as in previous years, no antitrust violations by Nornickel were identified, and no administrative action was taken for such violations by the antitrust authorities.

Information security

Nornickel's Information Security Policy applies to all employees and includes the engagement boundaries and responsibilities of the Board of Directors and the Management Board in this regard. Senior management's responsibilities include, among other things, reviewing information security risks and budgets for relevant programmes and projects. Risks are monitored on a regular basis through dedicated committees and corporate reporting.

In 2024, the Company faced new challenges prompting the need to refine existing approaches to information security management. To ensure consistent development, the information security function strives to improve its service model by aligning its approaches with best practices in the market. One of the function's key goals for 2025 is to boost the effectiveness of its key processes.

The Company's information protection strategy is built with consideration for both an increase in information security risks triggered, among other things, by continued geopolitical tensions and the government's ongoing drive to promote import substitution of information technologies and information security solutions. Specifically, in 2024, Nornickel completed the import substitution process for data protection tools used in industrial automation systems within the Company's technology infrastructure. Meanwhile, Nornickel has continued its efforts to substitute imports of corporate perimeter protection tools.

The Company is taking some extra steps to protect the technology infrastructure perimeters of its enterprises and mitigate the risks of production process disruption or shutdown.

With the Company still offering hybrid work schedules for office staff, the first stage of introducing two-factor authentication for employees was completed to minimise the risks associated with unauthorised remote access to corporate resources. The Company is continuously monitoring the security of its corporate systems to promptly identify and address vulnerabilities as well as prevent cyber intrusions.

To enhance the information security management system, in 2024, the Company developed and approved a model of corporate information security processes and implemented an information security process management system to aggregate information on key performance metrics. This has also enabled a high level of availability across information security services for internal customers within the service model, including through additional steps to boost protection against external cyber threats.

Risks related to cybercrimes against the Company's processes and systems as well as data privacy compliance risks are listed in the Company's corporate risk management system. The Information Protection and IT Infrastructure Department is the owner of these risks.

The Company's goals in building resilience to information security risks are set as KPIs for the department.

Certification

The information security management system (ISMS) in place at Nornickel enterprises complies with ISO/IEC 27001. The ISMS helps systematise and structure information security support processes while building an effective matrix of controls and ensuring timely risk identification and mitigation.

Five Nornickel enterprises are certified to ISO/IEC 27001:

- Transport Division in Murmansk
- Kola Site
- Nadezhda Metallurgical Plant
- Copper Plant
- Talnakh Concentrator

In 2024, activities aimed at transitioning site-level ISMS to ISO/IEC 27001:2022 were implemented to maintain cyber-defence processes at a high maturity level. The effectiveness of information security management processes across production sites was confirmed by audits. The external auditor noted strong management engagement in ISMS processes and the preparedness of the enterprises to respond to new threats and challenges. Employees involved in the operation of the ISMS showed excellent knowledge of information security.

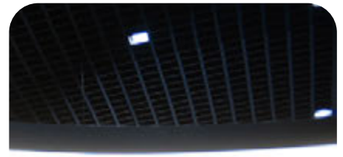
Security and vulnerability management

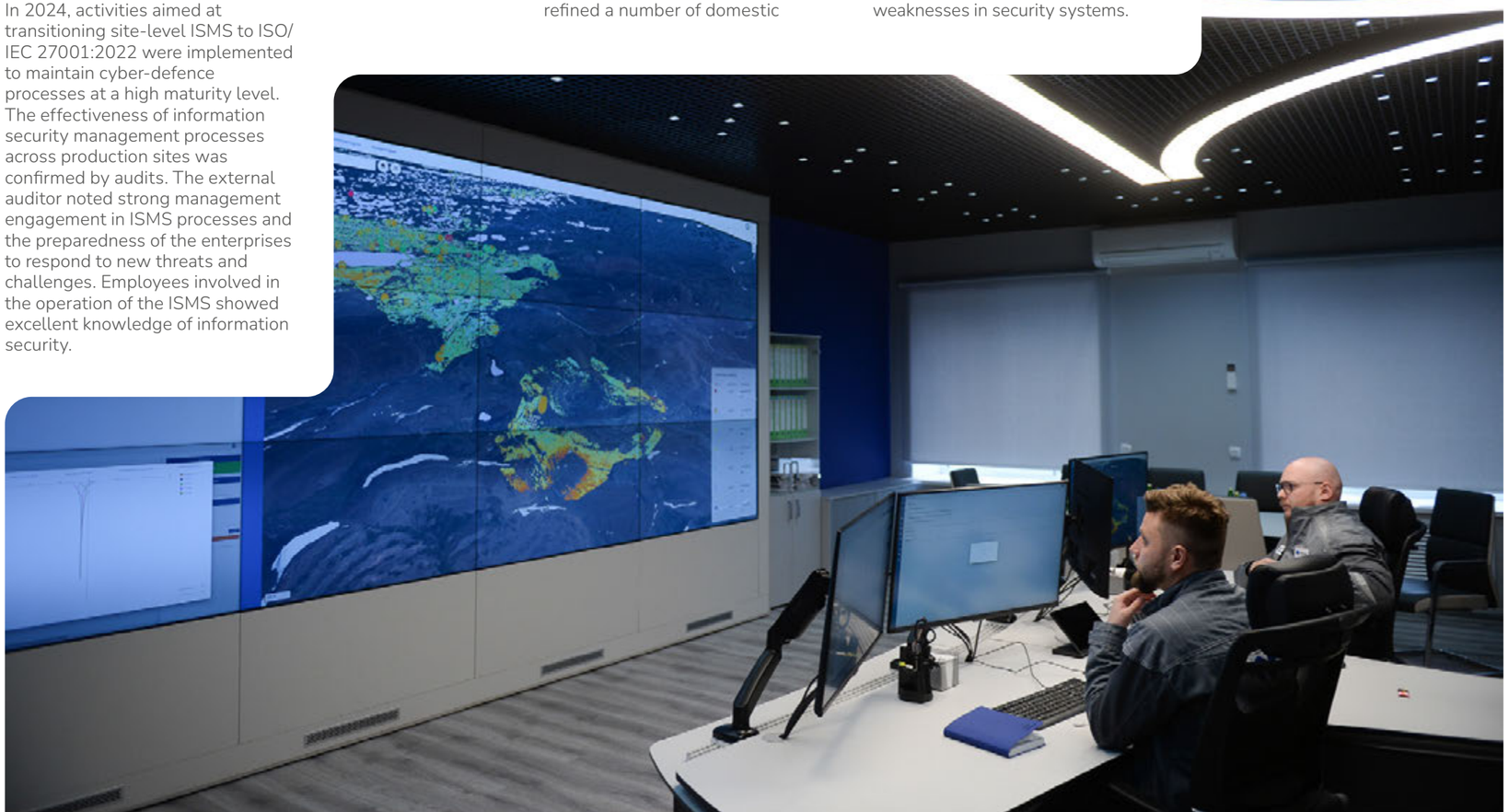
We have completed all activities planned for 2024 to boost the overall security of our automated process control systems (APCSs) and to implement audit recommendations from 2023.

The Energy Division's production enterprises completed their activities under the plan to implement basic process safeguards, significantly reducing information security risks at the facilities critical for the energy security of production enterprises as well as cities and towns in the Far North. In collaboration with key market partners, we have refined a number of domestic solutions offered by leading manufacturers of technological and production process automation systems and aligned them with Nornickel's information security requirements.

In 2024, the Company improved its approaches to managing vulnerabilities and conducting vulnerability analysis of corporate systems, with a special focus on APCS testing. Proven vulnerability scanning processes allowed us to identify weaknesses in existing systems, including in APCSs, and to take timely measures to bolster security. Regular penetration testing and conducting drills to improve coordination with the response centre team also help identify and address weaknesses in security systems.

The Company is actively engaged in developing security processes within the software development life cycle (SDLC). Deploying the DevSecOps methodology helps automate key security controls by integrating them directly into software development. To boost resilience to attacks targeting the supply chain, we have set up own repositories of libraries and components used in developing software products.





Cyber incident response system

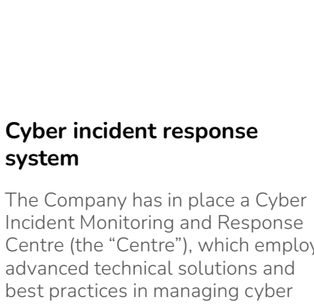
The Company has in place a Cyber Incident Monitoring and Response Centre (the "Centre"), which employs advanced technical solutions and best practices in managing cyber defence. Employees continuously improve their competencies and showcase them through competitions organised by partners. In 2024, the Nornickel team earned high marks and demonstrated unique competencies in three such competitions.

To maintain awareness about current information security threats, the Centre's employees continuously monitor information security events and regularly share information with colleagues from other companies and with market partners, enabling proactive measures to block malicious actions.

Despite a significant increase in cyberattacks in 2024, well-coordinated efforts allowed the Company to successfully repel all attempts by threat actors to damage Nornickel's infrastructure. In 2024, the Centre's employees addressed a total of almost 20 thousand information security events and about 1 thousand cyber incidents.

Company employees also help identify potential computer security incidents. Any employee detecting any suspicious content or activity on company devices can send an alert to the information security team for investigation. Experts assess the possible negative impact on the Company's information systems and take measures to prevent and eliminate the consequences of incidents. About 6 thousand investigations into incidents reported by Nornickel employees were conducted over the year.

Information security events handled



Requirements to counterparties

In 2024, cases of compromised IT infrastructure were identified for several contractors, with response measures taken immediately to block relevant contractors' access to Nornickel's infrastructure and prevent possible negative consequences.

Within the follow-up measures to address the associated risk, the Company developed a contract section outlining information security requirements and liability for non-compliance by counterparties getting access to Nornickel's data assets under relevant contracts. In 2024, this section was already added to the general terms and conditions for Company contracts.

The Information Security Requirements section was incorporated into contracts with counterparties that have critical access rights on Nornickel's IT infrastructure. In addition, the Company amended its standard confidentiality agreement / NDA to include the counterparty's obligation to ensure information security measures are implemented and to provide relevant details upon the Company's request.

To establish a holistic approach to handling information security risks associated with third parties, we are developing a methodology to evaluate Company counterparties on the adequacy of information security measures in place, with a view to enable extra defences for corporate data assets.

Personal data protection

To handle the risk of insufficient protection of customers' and employees' personal data, the Company has implemented and put in place a set of legal, organisational, and technical measures to ensure the security of personal data (PD). Technical protection of PD involves anti-virus protection, leak prevention, monitoring of removable devices, analysis of security incidents, etc.

In the context of greater liability for violations related to PD processing, the Company places a heightened emphasis on maintaining legal compliance of its personal data processing. The following initiatives were implemented in 2024, in line with the methodologies developed by the Information Protection and IT Infrastructure Department over 2024:

- At eight Nornickel enterprises, PD processing was aligned with relevant legal requirements and internal regulations
- Eleven Nornickel enterprises assessed their websites for compliance with legal requirements to PD processing

To reduce the risks of data leaks, the Company provides regular training to employees whose tasks include PD processing.

A methodology for lean PD processing has been developed to reduce the risk of PD leaks by minimising PD processing within business processes.

Training and communication

The Company is strongly focused on improving employee awareness about information security requirements and digital hygiene rules. In 2024, Nornickel set a goal to enhance information security culture across the entire Group.

The Company is driving initiatives to increase ownership of information security issues across the entire workforce, from the board room to the shop floor.

Information security issues are covered during mass corporate events and strategic sessions. Employees are updated about information security threats and digital hygiene rules via internal communication channels: publications on the intranet portal, mailings, corporate messenger, postings on bulletin boards, and videos on screens in common areas.

Nornickel provides regular training to employees on information security topics relevant to them, in particular through online courses updated to reflect changes in the threat landscape and relevant legislation. A total of 95 scheduled and 19 unscheduled trainings (including e-courses and face-to-face lectures) were held in 2024, where 34.8 thousand Group employees were trained.

To enhance employees' vigilance and practice the sequence of actions in case of an information security incident, the Company runs regular drills, including simulations of phishing attacks and other current unlawful practices that affect users. Following the drills, instructions for employees are updated.

A heightened emphasis is placed on the personal information security of Company employees and their family members, with activities designed and delivered for employees' children.

Information security training

Activity	2022	2023	2024
Number of trainings conducted, including:	70	114	114
scheduled trainings	*67*	*95*	*95*
unscheduled trainings	3	19	19
Employees trained	13,500	34,104	34,800

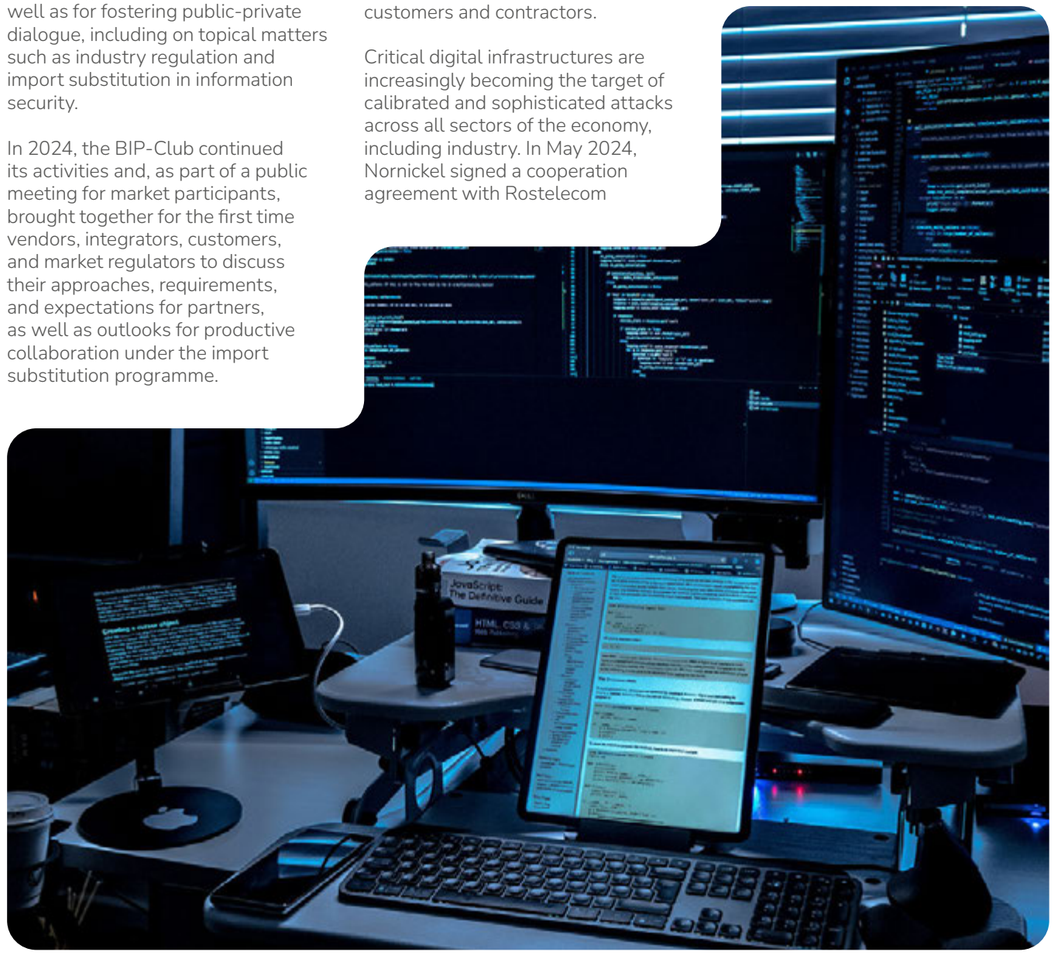
Partnerships

In 2017, Nornickel initiated the creation of the Information Security in Industry Club (BIP-Club), an association of chief information security officers of major Russian companies, which has evolved into a recognised platform for sharing experience and best practices in protecting information systems as well as for fostering public-private dialogue, including on topical matters such as industry regulation and import substitution in information security.

In 2024, the BIP-Club continued its activities and, as part of a public meeting for market participants, brought together for the first time vendors, integrators, customers, and market regulators to discuss their approaches, requirements, and expectations for partners, as well as outlooks for productive collaboration under the import substitution programme.

Nornickel is committed to contributing to the development of the information security market for the industrial segment. In particular, the Company used the BIP-Club to propose to the information security community a Code of Ethics for the information security market, containing a set of principles that will help improve the maturity of the market and foster better cooperation between customers and contractors.

Critical digital infrastructures are increasingly becoming the target of calibrated and sophisticated attacks across all sectors of the economy, including industry. In May 2024, Nornickel signed a cooperation agreement with Rostelecom to develop and improve solutions to prevent information leaks, control software security, and limit access to malicious information resources. Under the agreement, the two partners look to develop and implement solutions designed to improve cyber resilience of the metals and mining industry.



Independent audit

An independent auditor for Nornickel's financial statements is selected through competitive bidding in accordance with the Company's established procedure. The Audit Committee of the Board of Directors reviews the shortlist and recommends a candidate to the Board of Directors for approval at the Annual General Meeting of Shareholders of MMC Norilsk Nickel.

In 2024, based on the recommendation of the Board of Directors, the General Meeting of Shareholders approved Kept as the auditor for the Company's RAS and IFRS financial statements for 2024.

The Audit Committee of the Board of Directors, upon reviewing Kept's reports, raised no comments regarding the auditor's findings.

Auditor's fee

The fee paid to Kept for its audit services, auxiliary audit services, and other audit-related services in 2024 totalled RUB 280 million (USD 3.0 million), net of VAT, with the share of other audit-related services accounting for 36% of the total.

To prevent conflict of interest, Kept has a specific policy in place, covering different types of services they provide to auditees. This policy ensures compliance with the requirements of the International Ethics Standards Board for Accountants (IESBA), the Russian Independence Rules for Auditors and Audit Firms, and other applicable standards.

Auditor's fees

Service type	2022	2023	2024	
	RUB mln	RUB mln	RUB mln	USD mln
Audit services	116.9	125.8	133.9	1.4
Auxiliary audit services	57.3	36.7	44.3	0.5
Other audit-related services	165.6	69.7	102.0	1.1
Total	**339.8**	**232.2**	**280.2**	**3.0**