CHAPTER 9

Corporate governance

Risk management
and internal control

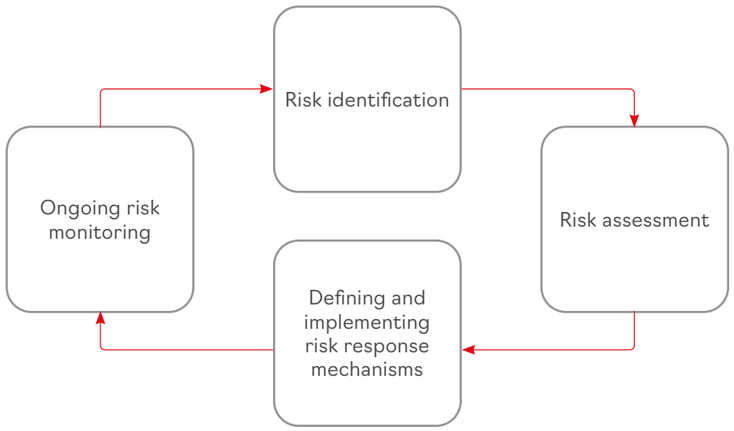
GRI 205-1

Magnit has an established system for managing financial and non-financial risks that forms part of an organization-wide internal control and risk management framework. Risk management is an ongoing and cyclical process. Managing non-financial risks is the shared responsibility of the management team and the Board of Directors.

The Internal Audit Department analyses and evaluates the risk management and internal control systems, as well as corporate governance.

The Corporate Governance Department performs the functions of the Corporate Secretary, ensures the efficient operation of the remaining corporate governance bodies and is responsible for all necessary disclosures.

Risk management consists of the following key elements



For Magnit, key risks are those that could have a material adverse effect on its operations, prospects or reputation. The Company identifies the following key sustainability risks:

Regulatory risk

Potential changes in environmental, talent management, health and safety regulations may have a negative impact on business. Experts closely monitor regulatory changes to mitigate regulatory risk.

Corruption and fraud risks

To manage these risks, the Company has in place a Code of Business Ethics and an Anti-Corruption Policy, operates a whistleblower hotline and reviews its work, participates in the UN Global Compact, and provides ethics and corporate conduct training to employees.

Epidemiological risks

Magnit closely monitors the spread of COVID-19, strictly follows all recommendations from national public health agencies (Rospotrebnadzor and the Health Ministry) and the WHO, performs regular disinfection of premises, and allows employees to work remotely.

HSE risks

Health, safety and environment (HSE) risks include disregard for occupational health requirements and fire safety rules, failure of contractors to comply with HSE requirements, etc.

Magnit provides HSE training to employees (with post-knowledge tests conducted by in-house HSE teams), participates in the UN Global Compact, performs regular checks of fire safety systems, ensures that employees have required competencies, has managers responsible for maintaining these competencies, performs workplace assessments, and observes the Environmental Protection and Occupational Health and Safety Policy and the Fire Safety Policy

Talent risk

Talent risk is the risk that the Company will face difficulties in retaining, sourcing or attracting qualified staff. This risk is managed by adopting comprehensive long-term incentive schemes and unique corporate training and adaptation programs, providing social and networking opportunities, teaming up with universities to attract top talent, and building a strong talent pool

Reputational risk

This risk includes the risk that the Company will not be able to maintain its reputation as a socially responsible business. Magnit has adopted a Sustainability Strategy, provides ethics and sustainability training to employees, and maintains an ongoing dialogue with all stakeholders

Climate risks

In 2021, we included climate risks in the overall risk management system of Magnit. In 2020, the Company conducted its first climate risk assessment using the "business as usual" (RCP 8.5) scenario whereby temperatures will rise by around 4°C by 2100. We analysed the impact on Magnit until 2050, identified risk mitigation actions and set clear GHG reduction targets. (for details, see Climate change and energy efficiency)

Tax Policy

Material topics

Creating
economic value

Priority SDGs

Key documents

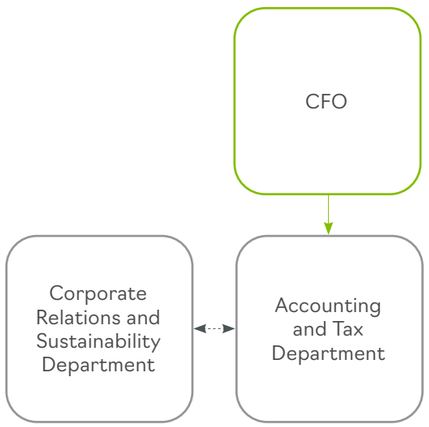
Magnit's policies and documents

- Tax Policy of Magnit
- Accounting Policy of Magnit

External documents

- Russian Tax Code and federal laws adopted in accordance therewith, Russian regional laws, laws and regulations on taxes and duties adopted by representative bodies of municipalities and executive bodies of various levels within the scope of their authority.

Governance structure



→ Administrative subordination
⇢ Coordination within the framework of sustainability reporting

Our approach to management

GRI 207-1, 207-2

As one of the largest taxpayers in Russia, Magnit helps generate budget revenues and contributes to the social and economic development of its business geographies and the entire nation. We support the territorial economic development and have a transparent tax policy. In 2021, the Company paid over RUB 122 bln in taxes, duties and insurance contributions to budgets of all levels and extra-budgetary funds in Russia.

As a responsible and diligent taxpayer, Magnit calculates and pays all applicable taxes, duties and fees in accordance with the Russian law and pursues a sound and consistent tax policy.

Tax policy goals

- Effective planning of tax liabilities and their scheduling in accordance with the applicable laws
- Monitoring and responding to changes in tax legislation and law enforcement practices
- Monitoring tax compliance to ensure high capital turnover
- Optimisation of tax costs

The principles of Magnit's tax policy

Integrity

We calculate and pay taxes based on the economic substance of operations and transactions and make use of tax incentives strictly in accordance with statutory requirements.

Uniformity

The Corporate Centre ensures uniform interpretation of tax legislation in accounting operations across different companies of Magnit Group and during the preparation of tax returns.

Transparency

We fully cooperate with the government agencies conducting tax audits and provide all necessary documents and reports as required by law.

Effective dispute resolution

In case of tax disputes, we seek to resolve them through pre-trial procedures envisaged by the law and bring the issue to court only as the last resort.

Reliability of counterparties

We scrutinise our counterparties and avoid doing business with the companies that are believed to be tax evaders or involved in tax avoidance schemes.

Tax risk management

Whenever there are uncertainties as regards interpretation of tax laws, we always ask government agencies for clarification. As a member of various industry associations, Magnit communicates its viewpoint on industry regulation and taxation to government officials.

Tax Policy
(continued)

The tax function is an integral part of Magnit's financial unit, ensuring that all of the Company's tax obligations are effectively discharged across its geographies. The overall financial management falls within the remit of our Chief Financial Officer.

The Deputy CFO heads the Accounting and Tax Department and is directly responsible for the tax function. The department's responsibilities include the following:

1. Tax accounting

2. Preparation and filing of tax returns

3. Cooperation with tax authorities during desk and on-site audits

4. Reconciliation of accrued and paid taxes

5. Identification of tax risks and their mitigation

6. Analysis of options for reducing tax liabilities, including incentives and preferences

7. Preparation of tax legislation initiatives

8. Development of internal policies, regulations and procedures.

The department is staffed with professionals who boast a great depth of expertise and relevant experience in this field. To raise our competencies, we engage external consultants from the Big Four accounting firms to deal with specific issues.

Stakeholder engagement

GRI 207-3

Our tax-related activities focus on timely compliance with tax regulations, including as part of tax audits conducted by tax authorities.

We actively cooperate with the Retail Companies Association (ACORT) in developing new tax regulations, assessing tax legislation amendments proposed by government agencies and adopting a stance on relevant initiatives aimed at improving the efficiency of the retail industry.

We expect full compliance with the tax legislation from Magnit's counterparties and monitor their activities to ensure that they are not involved in any tax avoidance schemes as a means to safeguard the Company against potential tax risks.

Tax risks and control

We continuously enhance our control procedures to increase the effectiveness of the tax function and tax risk management. Risks are managed through:

- implementing and maintaining an integrated system of internal tax controls;
- planning and controlling the pricing of intra-group transactions;
- monitoring the compliance of potential counterparties with the tax legislation when entering into transactions with them.

Tax payments

GRI 207-4

Tax data are regularly disclosed in the Company's consolidated financial statements. Magnit engages an independent auditor to confirm the reliability of its consolidated financial statements, including as regards the reported tax amounts and other tax data.

> RUB 122 bln
total tax payments, insurance contributions and duties

RUB 103 bln
Contributions to the federal budget: income tax, value added tax, and payments made to the budget on behalf of our employees, including personal income tax and contributions to the pension and health insurance funds

RUB 19 bln
Contributions to regional and local budgets: regional surtax on income tax, property tax, land tax, transport tax, and trade levy

Business ethics

and anti-corruption

Material topics

Business ethics
and anti-corruption

Priority SDGs

16 PEACE, JUSTICE AND STRONG INSTITUTIONS

UN Global Compact principles

№ 10

Key documents

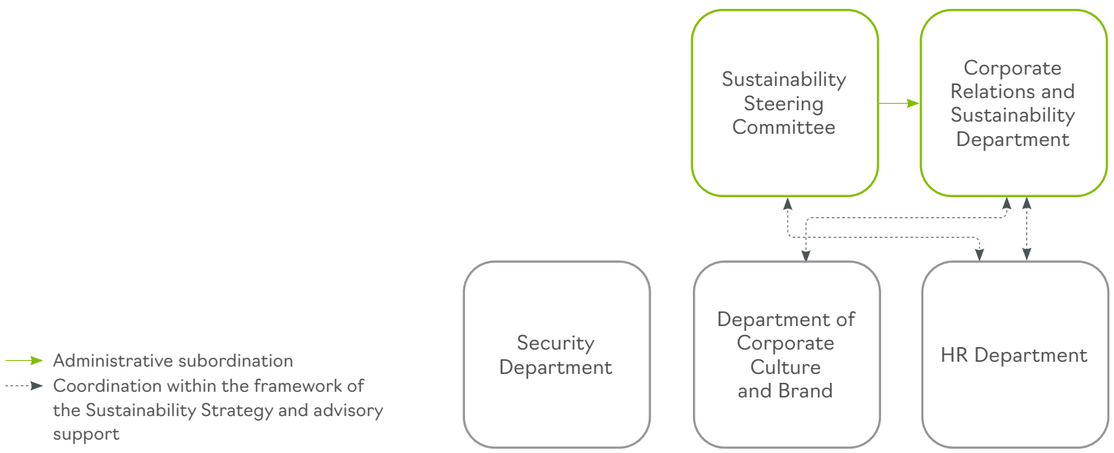
Magnit's policies and documents

- Business Ethics Code of Magnit
- Anti-corruption policy
- Regulation on the Anti-Corruption Hotline of the Anti-Corruption Policy of Magnit
- Contractual Policy of Magnit
- Internal Control and Risk Management Policy of Magnit
- Anti-corruption clause of the Anti-Corruption Policy of Magnit
- Regulation on Trade Secret of Magnit
- Regulation on Internal Checks of Magnit
- Internal Workplace Regulations of Magnit
- Tendering Policy of Magnit
- Regulation on Counterparty Due Diligence

External documents

- Criminal Code of the Russian Federation No. 63-FZ dated 13 June 1996
- Administrative Offence Code of the Russian Federation No. 195-FZ dated 30 December 2001
- Federal Law No. 152-FZ "On Personal Data" dated 27 July 2006
- Federal Law No. 149-FZ "On Information, Information Technologies and Information Protection" dated 27 July 2006

Governance structure



Our approach to management

GRI 205-1, 205-2

We maintain high legal, ethical and moral standards as part of our business activities and cooperation with business partners. These standards are set out in Magnit's Business Ethics Code, which is grounded in best Russian and international practices of business conduct, corporate governance and relationships with employees and other stakeholders.

Healthy human relations are at the core of every company, especially in the retail industry. The actions and decisions of any of our employees build and strengthen the Company's overall reputation. We seek to ensure that all our hires make honest and appropriate decisions based on the principles set out in the Code and follow the guidance that will enable us to meet the highest standards of business ethics.

Our zero tolerance approach to corruption in all its forms and manifestations provides the basis for the Anti-Corruption Policy, which underpins our corruption risk management system and our corruption prevention tools. Magnit's managers and employees should avoid being affected by any influences, interests, or relations that may have an adverse impact on the Company's business or facilitate any corrupt practices.

All new employees are required to attend courses on Business Ethics, Anti-Corruption Policy and Information Security, with refresher courses provided every three years.

All Company employees receive anti-corruption training after joining Magnit and are subject to control tests to check their acquired knowledge. In 2021, more than 166,000 employees completed anti-corruption training.

Underlying principles of the Anti-Corruption Policy

No.	Principle	Our responsibility
1	**Zero tolerance towards corruption**	Our Company is committed to zero tolerance of corruption in all its forms and manifestations, both on the corporate level and in stakeholder relations.
2	**Liability for corrupt practices**	We make every effort to promptly and indivertibly prevent any corrupt practices in accordance with the Company's by-laws.
3	**Senior management leadership by example**	Members of the Board of Directors, the Chief Executive Officer and other senior officers of the Company take a zero tolerance approach to corruption, establish and observe high ethical standards of business conduct and set an example to all Magnit employees.
4	**Corruption risk identification and assessment**	We identify and regularly assess the corruption risks relevant to the Company's operations, taking into account its strategic and investment development plans.
5	**Control procedures**	We have implemented control procedures to minimise corruption risks, including, but not limited to, checks of counterparties and addition of an anti-corruption clause to contractor agreements. We regularly assesses the effectiveness of our anti-corruption control procedures and takes steps to improve them.
6	**Counterparty checks**	To minimise reputational, financial and operating risks arising from relations with untrustworthy counterparties, we conduct thorough counterparty checks. We analyse information from open sources about the extent to which the counterparty adheres to ethical business principles and any anti-corruption practices it has in place, along with its willingness to comply with our principles and include anti-corruption provisions in agreements, as well as cooperate with a view to ensuring ethical business conduct and minimising corruption risks.
7	**Communication and training**	Our Anti-Corruption Policy is publicly available on the Company's website. We communicate anti-corruption principles and requirements to our employees, contractors, suppliers and other stakeholders. All our new hires go through mandatory anti-corruption training.
8	**Monitoring and control**	We regularly assess the compliance with anti-corruption procedures and communicate the results to the senior management and shareholders.

Business ethics and anti-corruption (continued)

Hotline

GRI 2-26

The Company maintains a 24/7 anti-corruption hotline for filing reports of corrupt practices and/or conflicts of interest occurring within the Company or on the side of counterparties. Each report is assigned a reference number with the date of receipt and the subject of the report. After the report has been received, a notification with its reference number and the date of registration is sent to the whistleblower to confirm that their report is being processed. Registered reports are assigned an ID, processed and registered by employees of the Department for Compliance and Antitrust Practices and the Economic Security Department for the purposes of further analysis and making appropriate management decisions.

All information submitted to the hotline is confidential and is not subject to disclosure except in cases stipulated by the relevant Russian legislation. The information that reaches the hotline can be accessed only by a limited number of employees who have received appropriate training.

The anti-corruption hotline is supervised by employees of Magnit's Department for Compliance and Antitrust Practices within the scope of their responsibilities. The manner, frequency and methods of performance evaluation are determined independently by the employees of the Department for Compliance and Antitrust Practices based on their professional judgement and experience.

24/7 hotline: 8 (800) 6000-477

Email: ethics@magnit.ru

Website feedback form:
https://www.magnit.com/ru/anti-corruption/

We guarantee that there will be no retaliation against any person contacting the hotline, including whistleblowers who report suspected acts of corruption committed by the Company's employees, no matter the circumstances.

Information security

Material topics

IT security

2021 highlights

- There were no confirmed incidents involving personal data of our stakeholders in 2021

Key documents

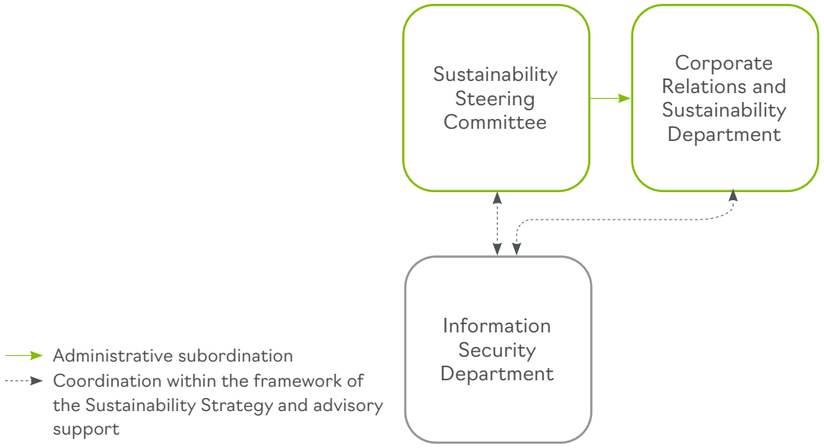
Magnit's policies and documents

- Anti-Virus Protection Policy
- Information Security Audit Policy
- Employee Information Security Awareness Policy
- Information Security Risk Management Policy
- Policy for Installing System Software Updates on Servers
- Regulation on Remote Access for Employees of Magnit Group's Companies
- Information Security Compliance Standard for Creating Information Systems and Services

External documents

- ISO 27001, an international information security standard developed jointly by the International Organisation for Standardisation and the International Electrotechnical Commission
- GOST R ISO/MEK 27001-2006 (Information technology. Methods and means of ensuring security. Information security management systems)
- Federal Law No. 152-FZ "On personal data"

Governance structure



Information security (continued)

Cyber security

Our approach to management

Magnit's information security is based on a set of interrelated organisational and technical tools which comprise an integrated information security management and assurance system. Our comprehensive approach enables us to protect ourselves against modern information security threats, comply with Russian legal requirements and international standards, and prevent financial, reputational and other damage. The Company's information security system is designed and developed in line with global best practices and the ISO 27000 series of international standards, and we are actively preparing for ISO 27001 certification.

Magnit has a formalised procedure for internal auditing, which falls within the remit of a dedicated department. We regularly assess information security risks and test our information systems on a quarterly basis.

Cyber security system

In line with our commitment to maintaining a cyber security system, we identify and eliminate vulnerabilities in information devices, search for viruses and zero-day attacks[1], while also monitoring and responding to security incidents. Additionally, Magnit monitors the integrity of software architecture across all of its external IT services. We carry out regular, scheduled updates of network devices, servers and software.

We carry out daily routine scans of all of the Company's external addresses for known vulnerabilities and eliminate all threats. All of Magnit's web services are protected through web application firewalls (WAFs), designed to detect and block network attacks on web applications. We actively employ Anti-DDoS[2] solutions, and regularly scan open internet ports. Upon the detection of an unauthorised port, our software automatically raises a red flag, and the connection is immediately checked. Every year, Magnit conducts an external independent vulnerability assessment of its IT system.

Development of IT security competencies

One of our information security priorities is to make employees more aware of cyber security rules. We lay particular emphasis on the training and professional development of the employees at our IT Department who ensure information security. Other departments working with IT systems in their day-to-day operations also hold regular trainings.

We seek to proactively and sufficiently train our employees working in various departments responsible for personal data processing. This became especially relevant during the pandemic when we introduced a hybrid work option.

Focus areas for raising employee awareness about information security

- safe operation of information systems
- corporate password policy
- detection of phishing and social engineering attacks
- the Company's information security standards

It was even before COVID-19 that the Company implemented a remote access system that enabled remote access to the corporate network for a number of employees whenever it was necessary, but this was done on a much smaller scale, with fewer simultaneous connections. Leveraging state-of-the-art technical solutions allowed us to quickly provide employees of all categories with stable and secure remote access to the corporate network. These activities became a priority for us amid the pandemic-related restrictions.

Our information security continues to improve as we are transitioning to a remote work format. For example, we are integrating security services to reflect corporate policies and provide users with a more advanced and convenient toolkit for remote work. Another major achievement that cannot be overlooked is the successful configuration of traffic control and assessment of users' devices security prior to their connection to the network, with further status updates to automatically respond to arising threats.

We strive to continuously improve our security systems to mitigate new threats; to this end, the Company has set the following targets for 2022:

- Introduction of a system for automatically assessing the security of information systems or networks by simulating an attack (a penetration test). The system is scrutinised for vulnerabilities that could cause the target to malfunction or to completely break down.
- Annual penetration tests for the Company's IT infrastructure and web services.
- Implementation of anti-fraud solutions in payment systems, accounting systems, B2B, and loyalty programmes.

[1] Zero-day – an exposed software vulnerability or malware with no identified means of containment
[2] Anti-DDoS is a tool of protection against DDoS attacks, which aim to disrupt the computer system through a constant stream of requests

Protection
of personal data

Our approach to management

We have developed a systematic approach to protecting the personal data of our stakeholders and continuously monitor the existing and planned information systems to ensure that personal data is processed appropriately and lawfully. Employees working with user data, including those in the IT Department, are duly trained, and persons charged with organising the processing of personal data receive regular briefings. We have developed consent forms for the processing of personal data, which are required to be filled by each employee, and appointed people responsible for organising and monitoring the data protection process. We believe it essential to raise awareness of information security, including personal data protection, among all our employees. We support and monitor business processes that require the processing of personal data as a means to safeguard the Company against possible sanctions from the government authorities. We also give guidance to experts from our subsidiaries on regulating the personal data processing matters

Magnit has an established procedure for reporting personal data breaches. We maintain a log of information security incidents in information systems for processing personal data; in 2021, no such incidents were reported. Furthermore, Magnit maintains a log of requests and enquiries regarding personal data from external stakeholders. In 2021, the Company received several enquiries and provided a reasoned response in writing within the deadlines stipulated in the relevant by-laws.

We carry out regular risk assessments as part of internal audits, as well as analyse processed data, develop and update threat models for information systems, design and implement technical solutions to eliminate such threats, and draft guidelines and regulations that help us comply with the laws on personal data.

Key documents

Magnit's policies and documents

- Personal Data Processing Policy
- Regulation on the Protection of Personal Data Processed by JSC Tander
- Regulation on the Officer in Charge of Organising Personal Data Processing
- Regulation on Handling Information Security Incidents in Information Systems for Processing Personal Data
- Regulation on Trade Secret
- Regulation on Classification of Information

External documents

- Federal Law No. 152-FZ "On Personal Data" dated 27 July 2006
- Federal Law No. 98-FZ “On trade secret” dated 29 July 2004
- Federal Law No. 149-FZ “On information, information technologies and information protection” dated 27 July 2006
- Presidential Decree No. 188 “On the approval of the list of confidential information” dated 6 March 1997