Risk Management

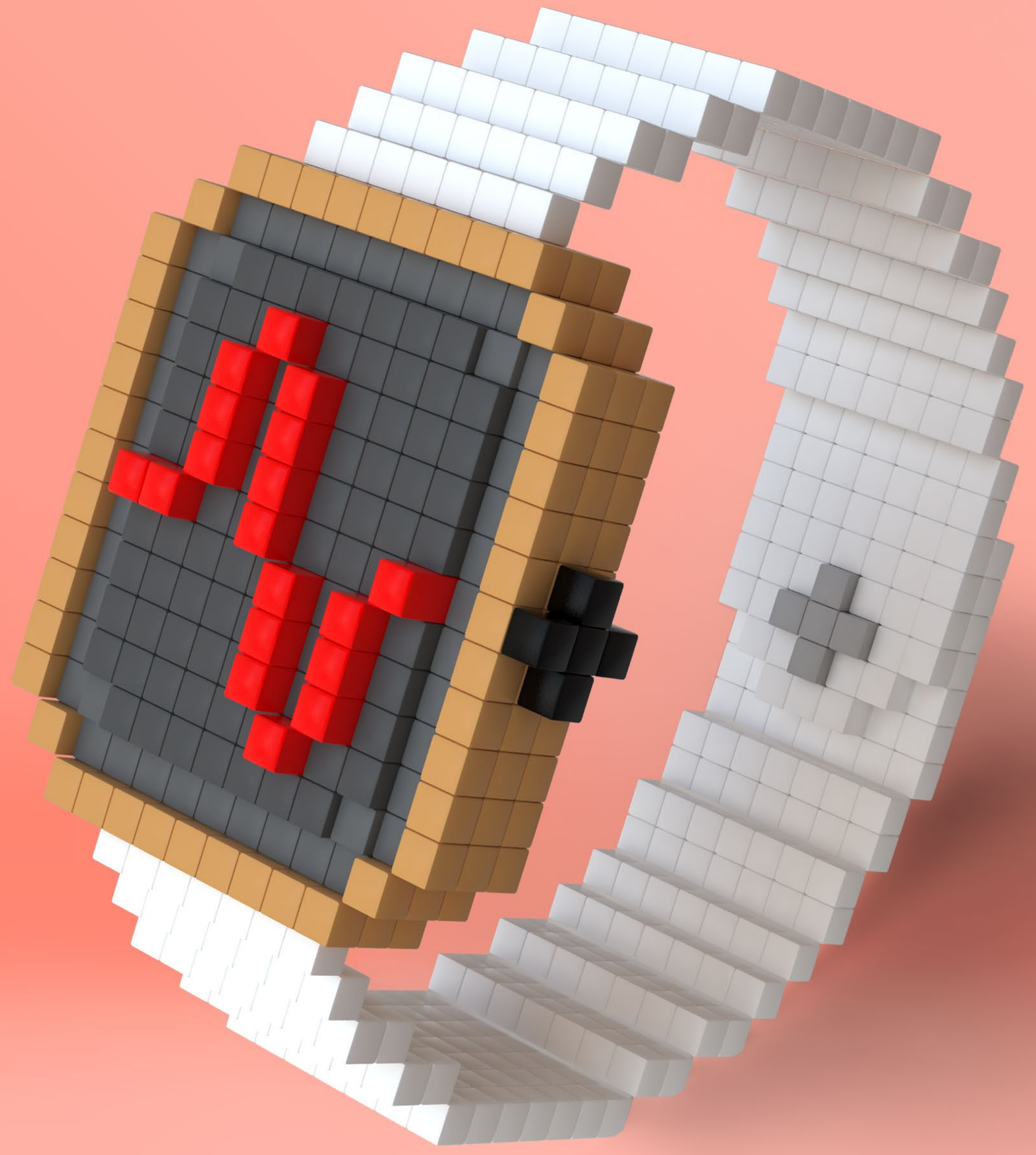
Rostelecom's risk management framework is deeply integrated into the Company's business processes and operates in full compliance with the requirements and guidelines of international and national regulatory bodies and agencies.

We promptly identify key risks and mitigate them and their potential effects.

Rostelecom assists the digital transformation of healthcare providers, contributing improvement opportunities in the quality and accessibility of their services.

3,134

Healthcare providers using our high-speed internet services in 2017



Risk Management Framework

Rostelecom takes a risk-focused approach to business decision-making both at a strategic and operational level.

Strategic risks are covered by the Risk Management Programme[69], which includes:

- a list of strategic lists, and strategic risk scenarios
- key strategic risk indicators and thresholds
- strategic risk management activities.

Operational risks are considered throughout our day-to-day operations, when developing new products and services, and in other Company projects. These risks are reflected in our project documents, standard risk registers, and scoring models for various business lines while also recorded in current reporting on business processes.

The Company's risk management framework has been designed and operates in full compliance with the requirements and recommendations of international and national risk management standards, and the guidelines issued by regulatory bodies and agencies[70] are additionally taken into consideration.

Rostelecom's key internal documents regulating risk management:

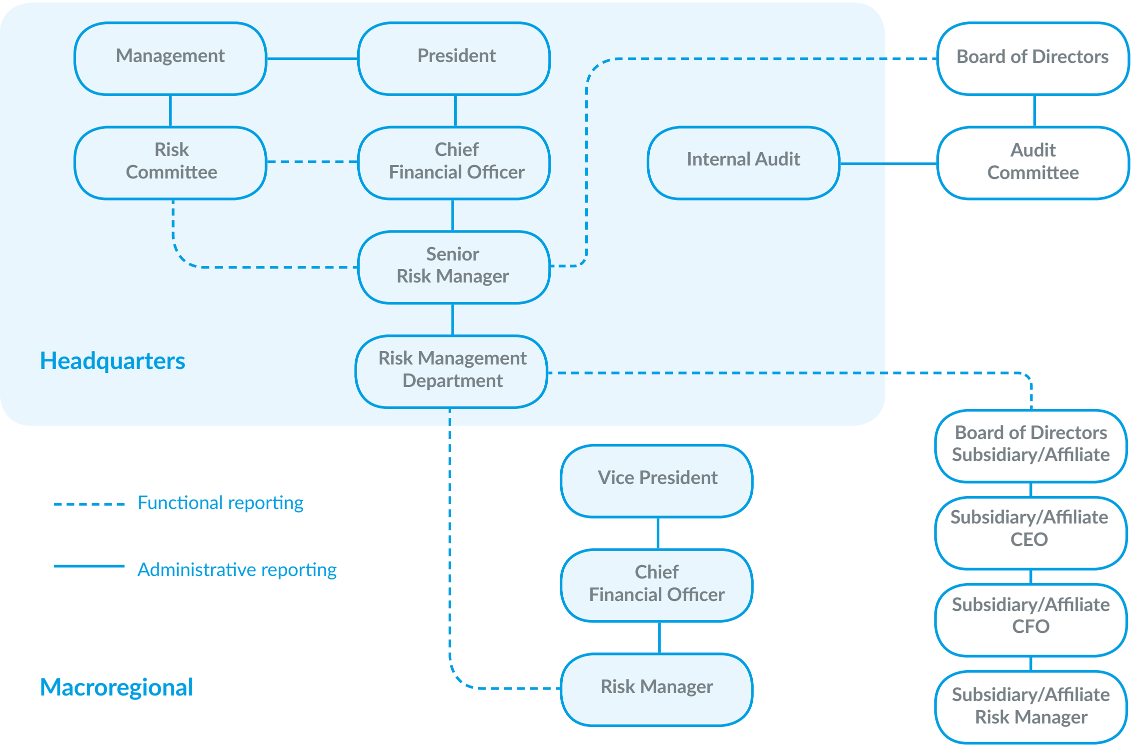
- Charter
- Risk Management Policy
- Regulations on the Board of Directors and Regulations on the Audit Committee of the Board of Directors
- Regulations on the Integrated Risk Management System
- Regulations on the Risk Management Committee of the Management Board
- Risk Management Procedure.

[69] Approved by the Board of Directors.
[70] GOST R ISO 31000:2010 Risk Management. Principles and Guidelines, Corporate Governance Code of the Bank of Russia, Guidelines for the Risk Management System Regulations issued by the Federal Agency for State Property Management, etc.

Risk Management Actors

Actor	Roles and responsibilities
Board of Directors	Defines the operating principles and improvement areas of the risk management framework; overall monitoring of risk management performance
Audit Committee	Supervises the operation of, and identifies gaps in, the risk management framework; makes recommendations to the Board of Directors
The Company's management	Manages key risks and regularly monitors the risk management framework
Internal Audit and Internal Control units	Assess risk management performance and advise on improvements
Senior Risk Manager and Risk Management	Build, monitor, and maintain the risk management framework[71]
Business units and employees	Manage risks within their areas of responsibility

Risk management interactions in Rostelecom Group



[71] For more details see the Corporate Governance section.

Risk Management in 2017

Rostelecom's risk management activities in 2017 were implemented as planned, allowing realised risks to be contained within the approved risk appetite and tolerance limits.

The Risk Management Committees held in-person meetings quarterly in 2017 at the Headquarters and macroregional branches to ensure effective risk management and improve risk management culture, and training in risk management was provided by Headquarters, macroregional branches, and our subsidiaries and affiliates.

In improving risk management performance, Rostelecom:

- devised a new method to calculate risk appetite and assess budget risks by simulating key financial metrics based on variance statistics for key contributing factors
- applied a new risk taxonomy based on seven common risk sources: market (customers and competitors), finance, legislation, IT, HR, technology, and counterparties
- implemented a key risk indicator model to identify and record variance and causes of variance in achieving monitored targets.
- updated its internal regulations governing the operation of the risk management framework, whereby revisions were made to the Regulations on the Risk Management Framework and the Risk Management Procedure
- introduced a top-down approach to preparing the Risk Management Programme – the 2018 programme was developed in the checklist format covering the risk scenarios identified based on the risk realisation trends for the Company during 2017 and relevant risks for 2018 in the telecommunications industry according to international experts.

In 2017, Rostelecom's risk management framework was certified to GOST R ISO 9001-2015 Quality Management Systems. Requirements.[72]

[72] Certificate of Compliance Reg. No. ROSS RU.IS79.K00122 dated 22 December 2017

Key Risks

Rostelecom's five biggest risks during 2017

2017 ranking	Risk	Risk description and potential impacts	Mitigation	Manageability in 2017
1	Lack of resources to ensure compliance with new legal requirements	The Company has to act pro-actively, accumulating funds in advance to ensure future compliance with the regulations coming into force in 2017–2018 (the Yarovaya Package, the Law On Security of Critical Information Infrastructure). Due to the lack of clearly specified requirements and required cost assessment, such pre-emptive response involves a significant risk.	» Assessing the size of investment required to ensure compliance with legal requirements » Monitoring regulatory changes » Collaborating with market partners; participating in industry working groups	Low
2	Unfavourable regulatory changes or breach of applicable legislation	The Company's activities are substantially regulated by government authorities; therefore any unfavourable changes in laws or other documents regulating certain services or business activities within the telecoms industry is a key legal risk	» Monitoring regulatory changes in the Russian Federation » Interacting with regulators » Developing mitigating measures	Low
3	Failure to realise expected benefits from lease or disposal of the Company's real estate assets	The Company owns multiple real estate assets, and the maintenance of some properties may cause losses. Contraction of the real estate lease/sale market may result in an unused surplus property vacated after the optimisation.	» Auditing service spaces » Pursuing flexible pricing policies » Vacating spaces in accordance with the access network upgrade programme	Medium
4	Unavailability or lack of demand for new products or services	Product launch delays or a misplaced focus when developing innovative products and services such as cloud-based services, IIoT solutions, geodata, IP VPN, TV, and MVNO may result in unmet targets for new services and projected revenues.	» Implementing new service development strategy » Using service development offices » Optimising our business process for new product development and roll-out	High
5	Accelerated decline rates in revenue from the MS service in the B2C segment due to mobile and IP substitution	Rostelecom continues to face increasing competition in the B2C segment of the Russian fixed-line services market, which may prevent the Company from retaining or growing its market share and customer base while potentially reducing its operating profit. The natural decline trend in the market for these services is due to subscribers changing their behaviours and moving towards new digital technologies.	» Upgrading telephony infrastructures » Implementing a set of measures to retain customers	Medium

Risk Management Plans

Rostelecom plans to further enhance its risk management framework in 2018 by:

- expanding the list of key risk indicators through joint effort with business process owners to regularly update the Risk Management Programme and monitor risks related to operations
- developing risk management skills and capabilities within the business
- fostering a risk management culture
- building effective risk management communications with the business, including between macroregional branches.

The risks that will remain relevant to Rostelecom into 2018:

- Underfinanced compliance
- Lower revenues from fixed-line
- Failure to meet launch deadlines for new products and services

Rostelecom Group's 2018 Risk Management Programme[73] also covers IT, cyber security and data integrity risks, which are the most significant risks for telecoms in coming years.

The principal risks for 2018 have been identified based on Rostelecom's updated strategy, risk event analysis covering 2017, and the forecasts by top international experts for key telecoms risks in 2018.

Key risks in 2018

Risk group	Change vs 2017	Risk (source)	Scenario	Manageability in 2017	Mitigation
Market risks	=	1. Slowed market recovery in terms of prices; price wars in some regions (customers) 2. Stronger trend in MS telephony revenue decline (customers, competitors) 3. Market capture by competitors (competitors)	1. B2C: Standstill of market recovery processes 2. B2C: MS revenue decline rate exceeding projections 3. B2C, B2B/G: Loss of competitive edge in new products due to longer time-to-market resulting from time-consuming procedures for new product integration into the current IT landscape	Medium	Customer loyalty building practices and integrated bundle offers Development of new services through product development offices
Financial risks	▼	4. Resource allocation in an environment of future TMT sector uncertainties	4. Lower project profitability due to unanticipated emergence of new entrants in the market during the project delivery period 5. Unmet project delivery schedules due to delayed approvals from external customers, vendors, or contractors 6. B2G: Higher receivables turnover due to late acceptance by public customers	Medium	Prioritising projects depending on applicable risk factors by project type Centralising claim management skills Focusing on risk criteria in project planning models Regular audits Improving approval, procurement, and project delivery control processes
Legal risks	=	5. Unfavourable regulatory changes and breach of law	7. Insufficient funds to finance compliance with law requirements coming into force in 2018 (Law On Security of Critical Information Infrastructure, the Yarovaya Package)	Low	Monitoring regulatory changes Collaborating with market partners; participating in industry working groups
IT	▲	6. Compromised data integrity or reliability (IT)	8. Increased cyber security incidents within Rostelecom's technical infrastructure 9. Higher volumes of data processing, data protection, data migration to cloud, or data management in various systems outstripping the pace of Rostelecom's internal IT systems integration	High	Implementing projects for cyber security and information protection of the network and internal services Prioritising internal IT systems development in line with target architecture implementation Acknowledging risks related to the criticality of internal and external services provided by the Company when running planning procedures

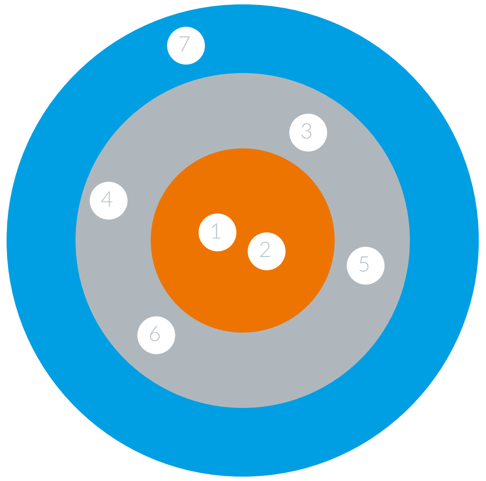
[73] Board of Directors' Minutes No. 12 dated 25 December 2017.

Key risks in 2018 (continued)

Risk group	Change vs 2017	Risk (source)	Scenario	Manageability in 2017	Mitigation
HR risks	▼	7. Insufficient key personnel (HR) 8. Personnel misconduct (HR)	10. Requirements of talented digital specialists and sales force in the B2B and B2G segments unmet by the workplace environment 11. Delays in project team staffing due to lack of personnel, unappealing vacancies, or inefficient recruitment 12. Personnel lacking in digital skills 13. Increased inquiries from supervisory and regulatory authorities due to Russia hosting major international events	High	Hosting events to improve brand perception Using modern talent search and recruitment tools Developing and using talent retaining tools Introducing new digital talent training tools
Technology risks	▼	9. Business interruptions due to key infrastructure outages (technology)	14. Outages in Rostelecom's networks reduced at a slower rate than the growth of infrastructure costs	High	Access network upgrade projects to reduce maintenance costs and outages; developing network outage monitoring systems Import substitution programme
Counterparty risks	▲	10. Market partners hijacking our M&A projects (counterparty)	15. Growing market competition for the highest-quality assets	Medium	Structuring the M&A process to optimise and speed up decision making on transactions

The risk scenario relevance was assessed through Monte Carlo simulations based on the Company's actual performance evolution in 2016–2017. The simulation captured the 44 most relevant factors affecting revenue and OIBDA by segment; the total variance is RUB 6.2 bn and RUB 4.5 bn respectively.

Rostelecom's risk radar 2018



● Critical risks
1. Market
2. Finance and planning

● Significant risks
3. HR
4. Technology
5. Legal
6. IT

● Moderate risks
7. Counterparty

Critical (market and financial) risks may result in failure to achieve KPI targets set in our Strategy and Long-Term Development Programme, as well as extended business interruptions, failure to meet obligations, significant downgrade of credit or corporate ratings, or negative publicity in national or international media.

Significant (legal, IT, HR, technology) risks may result in significant variance in key performance indicators, short-term business interruptions, downgrade of credit or corporate ratings, or negative publicity for the Company in regional or local media.

Moderate (counterparty) risks do not have a material impact on our financial and business performance; however they need to be monitored to ensure timely detection of their potential growth in materiality.