Risk Management

Rostelecom's risk management framework allows for effective modelling, assessment, and mitigation of risks that the Company is exposed to. The framework is structured in full compliance with the requirements of international and national regulatory bodies. To further enhance its reliability, Rostelecom implements projects aimed at automating risk management processes.

Risk management framework

Rostelecom's risk management framework emphasises effective management decision-making under uncertainties and related risks and capturing identified opportunities to achieve strategic goals.

Risk management is carried out in full compliance with international and national standards. The Company updates its risk management regulations as a part of business-as-usual.

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

Risk management is based on a system of concise, clear, and measurable corporate goals set by Rostelecom shareholders and management. Rostelecom approves its Risk Management Programme every year and monitors its execution on a quarterly basis.

Risk Management Programme includes:

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

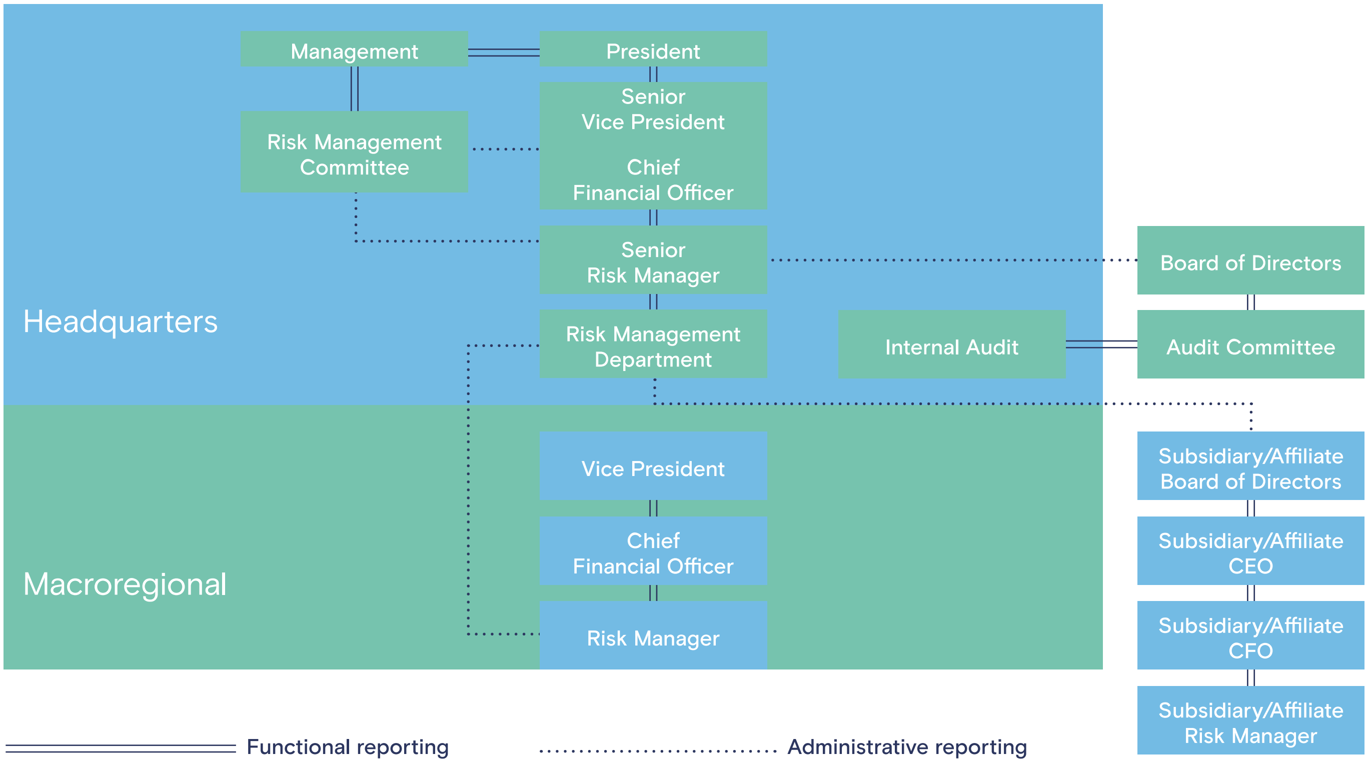
Operational risks are considered throughout our day-to-day operations and when developing new products and services. To ensure risk monitoring and rapid decision-making, Rostelecom develops and automates risk dashboards for business processes. In particular, Rostelecom developed an automated risk dashboard for procurement in 2018.

Quarterly progress reports on the Risk Management Programme and other relevant matters are reviewed at the meetings of the Management Board's Risk Management Committee which approve follow-up risk management initiatives.

RISK MANAGEMENT ACTORS

Actor	Roles and responsibilities
Board of Directors	Defines the operating principles and improvement areas of the risk management framework; performs overall monitoring of risk management performance
Audit Committee	Oversees 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 units	Build, monitor, and maintain the risk management framework
Business units and employees	Manage risks within their areas of responsibility

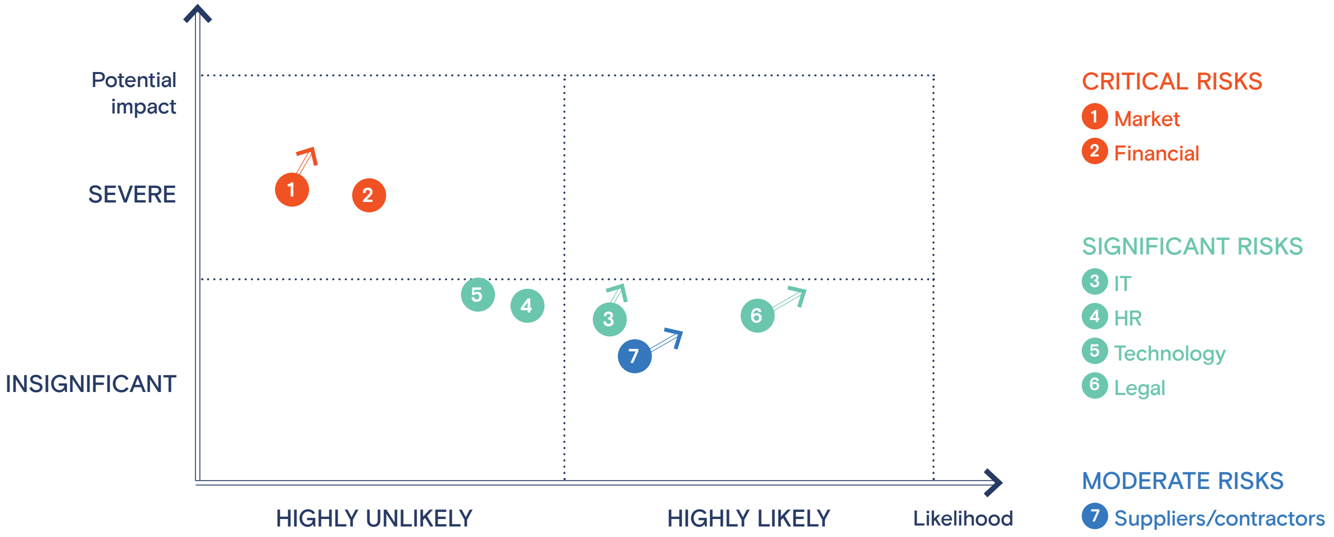
FIG. 21. RISK MANAGEMENT INTERACTIONS WITHIN ROSTELECOM GROUP



Rostelecom Group's risks

The risk map details the key risks Rostelecom is exposed to. Dots show the severity of potential impact and risk likelihood in 2018. Arrows show risk movement forecasts for 2019.

FIG. 22. RISK MAP



Critical risks may result in:

- failure to achieve KPI targets set in our Strategy and Long-Term Development Programme
- extended business interruptions
- significant downgrade of credit or corporate ratings
- negative publicity in national or international media.

Significant risks may result in:

- significant variance in key performance indicators
- short-term business interruptions
- downgrade of credit or corporate ratings
- negative publicity for the Company in regional or local media.

Moderate 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.

Development of the risk management system in 2019 will prioritise:

- identifying risks and developing mitigating measures
- deploying advanced risk management solutions
- automating risk dashboards for business processes to enable prompt notification of management.

TABLE 7. RISKS AND MITIGATION

No.	Risks in 2018	Mitigation in 2018	Manageability in 2018	Change in manageability in 2019	Risks in 2019	Mitigation plans for 2019
1	**Market risks** 1. Slowed market recovery in terms of prices; price wars in some regions 2. Stronger trend in MS telephony revenue decline 3. Market capture by competitors	Development of new products and services Measures to improve customer loyalty Measures to ensure reduced time-to-market for new products to capture market share	Medium	↑	**Market risks** 1. Flat ARPU 2. Higher subscriber churn 3. Market capture by competitors	Measures to improve customer loyalty Development of new services through product teams
2	**Financial risks** Resource allocation in an environment of future TMT sector uncertainties	Automation of procurement violations monitoring to enable prompt notification of management and reduce business impact during control procedures Procurement regulations updates	Medium	=	**Financial risks** Insufficient funds to invest in business growth	Prioritising projects depending on applicable risk factors by project type Focusing on risk criteria in project planning models Regular audits Improving approval, procurement, and project control processes
3	**IT risks** Compromised data integrity or reliability	Prioritising IT projects Aligning the development of business continuity management projects with integrated information security system for target OSS/BSS architecture Implementation of information security measures	High	↑	**IT risks** Compromised data integrity or reliability	Implementing projects for cyber security and information protection of the network and internal services Prioritising improvements to internal IT systems Acknowledging risks related to the criticality of internal and external services provided by the Company when running planning procedures

No.	Risks in 2018	Mitigation in 2018	Manageability in 2018	Change in manageability in 2019	Risks in 2019	Mitigation plans for 2019
4	**HR** Key personnel shortages Personnel misconduct	Providing comfortable working environment and development opportunities for employees Using modern talent search and recruitment tools Developing and using retaining tools	High	=	**HR** Key personnel shortages Personnel misconduct	Improving employer brand Using modern talent search and recruitment tools Developing and using retaining tools Introducing new training tools
5	**Technology** Business interruptions due to key infrastructure failures	Improving reliability and developing the network infrastructure	High	=	**Technology** Business interruptions due to key infrastructure failures	Access network upgrade projects to reduce maintenance costs and failures; developing network failure monitoring systems Import substitution programme
6	**Legal** Unfavourable regulatory changes	Monitoring regulatory changes Assessing equipment requirements and drafting a list of initiatives required to comply with applicable laws and regulations Assessing investment requirements of approved initiatives	Low	↑	**Legal** Unfavourable regulatory changes	Monitoring regulatory changes Cooperating with market partners; participating in industry working groups
7	**Suppliers/contractors**	New risk included in the Risk Management Programme	High	↑	Missed deadlines, overpricing, low quality of services and work performed by suppliers or contractors	Improving approval, procurement, and project control processes