CRITICAL RISKS

The key parameters of the Risk Management System annually approved by the Board of Directors of the Company serve as the basis for classifying a risk as critical. During the prioritisation, each risk is assessed according to two scales, the damage assessment scale and the risk probability assessment scale. Damage assessment implies that a risk is evaluated by its possible financial consequences and by its potential industrial safety impact, with the worst-case scenario taken as the risk impact score. The resulting estimates are then compared with the matrix for classifying risks as critical.

The 2018 list of critical risks was approved by the Board of Directors of Transneft[1]. In 2018, the register of risks was updated for further prioritisation and adoption of the list of critical risks for 2019. The risks were prioritised by the resolution of the Risk Management Council dated 10 October 2018 (Minutes No. 6). The list of critical risks for 2019 was approved by the resolution of Board of Directors of Transneft dated 11 December 2018 (Minutes No. 19).

Appointed for each of the Transneft critical risks is a risk owner who determines and authorises a business unit to manage the given risk, decides on the key risk indicators to monitor the risk dynamics and approves an action plan to manage the critical risk developed by the authorised business unit. The register of risks is revised annually, with special reporting on critical risks being generated.

Amendments to the List of Critical Risks

Critical Risks in 2018	Critical Risks in 2019
▪ Currency exchange and interest rate risks ▪ State regulation of oil and petroleum products transportation tariffs ▪ Fiscal risks ▪ Unlawful interference including terrorist attacks or attempts ▪ Shutdown of external power supply to Transneft's facilities ▪ The risk of changes in regulatory documents and legal acts setting and regulating technical requirements ▪ The risk of a partner bank's license being revoked ▪ International sanctions	▪ State regulation of oil and petroleum products transportation tariffs ▪ Fiscal risks ▪ Unlawful interference including terrorist attacks or attempts ▪ International sanctions ▪ Credit risk concerning partner banks ▪ Shutdown of external power supply to Transneft's facilities ▪ The risk of changes in regulatory documents and legal acts setting and regulating technical requirements

Critical Risks Management at Transneft in 2018

Possible consequences	Measures taken to reduce risk materialisation probability and mitigate the consequences of materialised risks	Actual materialisation of risks in 2018
1. Currency exchange and interest rate risks *Changes in interest rates on loaned funds and changes in currency exchange rates*		
Unbudgeted costs related to foreign currency loan services	▪ Analysis and evaluation of currency exchange and interest rate risks ▪ Monitoring and review of currency exchange and interest rate risks ▪ Use of currency exchange and interest rate risk management tools ▪ Monitoring of the efficiency of currency exchange and interest rate risks management	The partial risk materialisation in 2018 did not substantially affect the Company's financial performance. Full early repayment of the debt on the Loan provided by the China Development Bank (CDB) and timely repayment of Eurobonds in 2018 resulted in a significant reduction in currency exchange and interest rate risks
2. State regulation of oil and petroleum products transportation tariffs *Restrictions on oil and petroleum products transportation tariffs below the level required for the development of the Transneft system or below the level required to ensure reliable operation of the Transneft system in the long term. Dependence of petroleum products transportation tariffs upon the Russian Railways tariffs and the changes in them for the same transportation routes, which, in its turn, affects the tariff-based revenue of the Company*		
Project schedule slips. Reduced efficiency on certain transportation routes. Insufficient revenue to cover the costs required for maintenance of the reliability of the Transneft system	▪ Interaction with the Federal Antimonopoly Service (FAS) of Russia on the matters of scheduled (or, where necessary, unscheduled) review of oil and petroleum products transportation tariffs as well as in setting and abolishment of oil and petroleum products transportation tariffs. ▪ Interaction with the FAS of Russia in setting (review, abolishment) of approved oil and petroleum products transportation tariffs ▪ Interaction with federal executive authorities on deregulation of prices for petroleum products transportation	The risk partially materialised in 2018: pumping tariffs were set below the expected level. The impact on the revenue of the Company does not exceed the preferred risk level

[1] *Approved by the resolution of the Board of Directors of Transneft dated 27 December 2017 (Minutes No. 20).*

Possible consequences	Measures taken to reduce risk materialisation probability and mitigate the consequences of materialised risks	Actual materialisation of risks in 2018
3. Fiscal risks		
Changes to tax, customs, social security, and pension insurance laws and regulations		
Unbudgeted costs, claims by tax authorities	▪ Determining the level of tax burden on revenue ▪ Tracking changes in the tax law, studying bills submitted to the State Duma ▪ Monitoring of specialised press and other information resources ▪ Monitoring the legislation and arbitration practices ▪ Adjusting budget items, based on changes to the law, taxation, customs regulations, social and pension insurance ▪ Analysing certain aspects of operational activities and projects for taking tax risks into account ▪ Adjusting the accounting policy and other methodological documents ▪ Collecting information on the number of tax disputes and the sum in dispute	The partial risk materialisation in 2018 did not substantially affect the Company's financial performance
4. Unlawful interference including terrorist attacks or attempts		
Wrongful action (inaction) threatening safe operation of a fuel and energy sector (FES) facility. Threat of attack (or actual attack) on the line facilities of Transneft and its subsidiaries. Threatening calls ("telephone terrorism") and other acts that may entail significant disruption of the operation of the Company's security facilities. Illegal tapping into oil trunk pipelines and petroleum products pipelines. (Except cybersecurity issues related to risk 2017-24)		
Disruption of oil and petroleum products pipeline transportation facilities and power supply, control, automation and communications systems	▪ Making a list of TPs' facilities protected by departmental security ▪ Organising and controlling the process of classification of Transneft subsidiaries' facilities in need of protection and drafting security certificates for fuel and energy sector facilities ▪ Organising control over security units of Transneft subsidiaries and Transneft Security Services to address the challenges of assuring security at TP facilities ▪ Assessing the state of technical security equipment and the degree of antiterrorist protection at the facilities belonging to Transneft subsidiaries ▪ Ensuring the involvement of Transneft subsidiaries' security units and Transneft Security Services in the Neft-GSM investigative and preventive measures taken by the Ministry of the Internal Affairs of the Russian Federation ▪ Monitoring the implementation of the plans for additional measures to ensure antiterrorist protection of facilities and personnel of Transneft subsidiaries developed by Transneft subsidiaries to match the terror threat levels established by Russian laws ▪ Executing Presidential Decree No. 202 of 9 May 2017 "On the Specifics of the Use of Enhanced Security Measures during the 2018 FIFA World Cup in the Russian Federation and the 2017 FIFA Confederations Cup" ▪ Executing the resolution adopted at the meeting of the task force for counterterrorism at FES facilities under the Ministry of Energy of Russia (Minenergo) convened on 22 May 2018 to discuss the issue of Implementation of Mandatory Requirements and Tightened Security, Including Counterterrorism Measures, to Ensure Safety at Fuel and Energy Facilities in the Regions where FIFA World Cup 2018 will take place (Minutes No. 13-477 of 22 May 2018, Section 4, Clause 3) ▪ Organising meetings of the Anti-Terror Security Commission of Transneft and its subsidiaries ▪ Complying with decisions of the Anti-Terror Security Commission of Transneft and its subsidiaries ▪ Implementing the resolutions of the Government Commission on Electricity Supply Security (Federal Headquarters) (Minutes No. 10-2017 of 27 December 2017) in terms of security and antiterrorist protection of fuel and energy facilities ▪ Implementing the resolutions of the interagency task force for counterterrorism at FES facilities under Minenergo (Minutes No. ChA-55rg of 7 November 2018) ▪ Improving the regulatory framework in the field of security and antiterrorist protection of fuel and energy facilities ▪ Implementing measures to increase the protection level at TP facilities in case of aggravation of the situation, as well as on weekends and public holidays ▪ Arranging drills and trainings at Transneft's and Transneft subsidiaries' facilities protected by departmental security services ▪ Detecting and identifying persons from among the staff of Transneft subsidiaries and contractor (subcontractor) organisations intending and / or attempting to commit a terrorist act for the purpose of unlawful interference in the operations of the Company's TP facilities and the facilities belonging to Transneft subsidiaries.	The partial materialisation of the risk had no impact on implementing the plan in the field of oil / petroleum products pumping

Possible consequences	Measures taken to reduce risk materialisation probability and mitigate the consequences of materialised risks	Actual materialisation of risks in 2018
5. Shutdown of external power supply to Transneft's facilities *Interruption of external power supply to the Company's facilities through no fault of "in-house" reasons*		
Pipeline downtime. Unbudgeted costs. Emergency	▪ Transneft subsidiaries coordinating requests for changing the operational condition of electrical equipment in keeping with OR-03.100.50-KTN-170-15, based on the analysis of the operation mode of the adjacent grid ▪ Updating Transneft subsidiaries on the decreased reliability of power supply, based on the analysis of monthly maintenance and repair schedules for 220-500 kV class power supply equipment ▪ Cooperating with Rosseti to inspect overhead transmission lines (OTL) providing external power supply to Transneft subsidiaries' facilities	The partial materialisation of the risk in 2018 had no impact on implementing the plan in the field of oil / petroleum products pumping
6. The risk of changes in regulatory documents and legal acts setting and regulating technical requirements *Changes in the statutory and regulatory requirements in the field of technical regulation (including environmental requirements and requirements to operation of hazardous operating facilities)*		
Unbudgeted costs. Suspension of operations. Project schedule slips	▪ Monitoring of bills and other draft laws and regulations (LAR) published on the Federal LAR portal and establishing (governing) technical requirements affecting the Company's operations	The risk did not materialise in 2018
7. The risk of a partner bank's license being revoked *Suspension of operations or revocation of a partner bank's license*		
Financial and reputational losses, delayed contract settlements	▪ Emergence of limits to transactions with partner banks ▪ Monitoring of compliance with the set limits ▪ Monitoring of partner banks' creditworthiness	The risk did not materialise in 2018
8. International sanctions *Foreign economic restrictions, embargoes, freezing of accounts and settlements, US extraterritorial sanctions*		
Ban on the import of necessary equipment into the Russian Federation. Disruptions in supply of imported components; Restrictions on settlements with foreign counterparties; Restrictions on access to international markets	▪ Participation in the development of a comprehensive response to restrictive measures at the state level (including through intergovernmental committees / combined intergovernmental committees, business councils and field-specific panels and committees) ▪ The process of finding, establishing, and developing contacts with relevant influencer agencies abroad and identifying opportunities for to circumvent restrictions ▪ Development of proposals for gaining access to services and technologies through neutral or friendly jurisdictions, or alternative suppliers ▪ Monitoring and analysis of draft laws and regulations and laws that have been passed as well as official press releases of US and EU departments in charge of sanctions	In 2018, there were no changes to the sanctions regime with respect to Transneft

According to the results of prioritisation, the prospects for 2019 have not changed for most of 2018 critical risks, except the Currency Exchange and Interest Rate Risks. Its estimated damage decreased substantially, which led to its removal from the 2019 Critical Risks List. Such a change is attributable, first of all, to a reduced foreign currency exposure of the Company, due to early repayment of the debt on the loan provided by the China Development Bank, among other things. This also resulted in mitigated impact of floating interest rates pegged to LIBOR on the Company.

Specific Risks. Cybersecurity Risks

Cybersecurity is one of the priorities of Transneft's and Transneft subsidiaries' activities. Transneft is guided by a long-term Programme for Combating Threats to Information Technology Resources. The programme provides for improvement of detection, prevention and mitigation of computer attacks including those aimed at facilities belonging to the critical information infrastructure and response to information security incidents, as well as for the introduction of a package of cybersecurity solutions.

According to Russian laws, Transneft Group companies are critical information infrastructure (CII) subjects.

One of the priorities at Transneft Group is to ensure safe and uninterrupted operation of the information infrastructure and the information technologies used in the automation of technological and business processes, protection of trade secrets and other confidential information.

Management Approach

Transneft Group implements the Information Security Policy, which defines the key objectives in the field of information security, including:

- Protecting Transneft's and Transneft subsidiaries' personnel from pain, suffering and loss of amenity and other damages resulting from unlawful use of information relating to them, including personal data
- Protecting and maintaining Transneft's and Transneft subsidiaries' positive image and business reputation
- Ensuring continuity of technological and business processes
- Supporting innovation-based and boosted development of information security and information technologies
- Minimising possible damage from realised information security threats.

Documents

- Federal Law No. 98-FZ dated 29 July 2004 On Commercial Secrets
- Federal Law No. 149-FZ dated 27 July 2006 On Information, Information Technologies, and Information Protection
- Federal Law No. 187-FZ dated 26 July 2017 On the Security of the Critical Information Infrastructure of the Russian Federation and regulations thereunder
- Decree of the President of the Russian Federation dated 15 January 2013 No. 31s On Establishing of a State System for Detection, Prevention, and Response to Computer Attacks on Information Resources of the Russian Federation
- Decree of the President of the Russian Federation dated 5 December 2016 No. 646 On Adoption of the Information Security Doctrine of the Russian Federation
- Transneft's Information Security Policy approved by the Board of Directors, Minutes No. 21 dated 28 December 2017
- Programme for Combating Threats to Information Technology Resources (implementation period: 2017 to 2020)

Countering Cyber Threats

Transneft's information technology resources are target of an increasing number of hacker attacks. In 2018, about 7 million emails with inappropriate content allowing for malicious software installation were processed. During the reporting year, there was an increase of the share of emails labeled as "virus" in the mail traffic. This fact partially testifies to the growing phishing activity recorded in the world. The number of attempted computer attacks on Transneft's data processing centre also increased.

In 2018, measures were taken under the Programme for Combating Threats to Information Technology Resources of Transneft (hereinafter, the Programme) and the IT resources of Transneft subsidiaries, aimed at:

- Providing for and supporting of the activities of the Computer Security Centre
- Providing for interaction with the Russian State System for Detection, Prevention, and Mitigation of Computer Attacks (GosSOPKA)
- Establishing a centralised system for monitoring and controlling information security events, allowing for taking stock of IT resources, collection and correlation of information security events and response to information security incidents
- Providing for interaction with consumers of oil and petroleum products transportation services for mutual informing about computer attacks
- Conducting R&D activities in the field of cybersecurity

A regulatory and methodological framework for classification of CII facilities was developed at Transneft in order to comply with the requirements of Russian laws governing the security of CII facilities, and relevant events were implemented.

Plans for 2019

In 2019-2020, implementation of the Programme will be focused on ensuring secure interaction between Transneft's and Transneft subsidiaries' corporate computer network and the Internet, and on raising the information security awareness of the personnel.

Completion of measures for classification of CII facilities, identification of significant CII facilities, and ensuring the implementation of the procedures required for their protection.