Risks of Rosseti Centre, PJSC for 2026
with significant and critical levels of materiality

Item #	Risk ID	Risk category	Risk name	Level of risk materiality (final risk assessment)	Risk management measures
1	2	3	4	5	6
1	SR 1	Strategic risks	Failure to achieve indicators of the level of reliability of power supply	Significant	1. Formation of maintenance and repair programs taking into account the results of assessment of the current technical condition of equipment, including those performed based on the results of diagnostics of electrical grid equipment 2. Monitoring the quality of maintenance and repair (including those performed by contractors) 3. Timely renovation of the grid and targeted programs to improve reliability (execution of the investment program) 4. Organizing control over the implementation of measures based on the results of the investigation of technological violations (failures) 5. Development and updating of provisions on technological interaction with related subjects of the electric power industry 6. Improving the quality of work with personnel: hiring, training, advanced training
2	OR 2	Operational risks	An accident at work	Critical	1. Implementation of measures of the Comprehensive Industrial Safety Program of Rosseti Centre, PJSC for 2026-2028
3	OR 3	Operational risks	Failure to achieve readiness for work during the heating season	Significant	1. Monitoring the implementation of activities of supervisory authorities 2. Monitoring special performance indicators 3. Monitoring reporting during preparation for the heating season 4. Timely planning and implementation of measures based on the results of inspections by state supervisory authorities (Rostechnadzor, Ministry of Energy, etc.)

4	OR 9	Operational risks	Violation and (or) termination of the functioning of critical information infrastructure facilities as a result of computer attacks	Significant	1. Implementation of organizational and technical measures in accordance with the requirements of the legislation of the Russian Federation in the field of information security: practical implementation of measures to create a comprehensive information security system within the framework of the Information Security program 2. Regular monitoring of the measures taken to protect information at the Critical Information Infrastructure facilities: checking the settings of the information security system; conducting inspections of compliance with requirements of local regulations on information protection; updating the local regulations in accordance with the requirements of legislation in the field of information security
5	LR 1	Risks of violating the law	Violation of antimonopoly legislation	Significant	1. Analysis of compliance by the Company/an employee of the Company with antimonopoly legislation 2. Measures in accordance with the Company's Policy in the field of Antimonopoly Compliance (antimonopoly policy)
6	LR 9	Risks of violating the law	Commitment of a corruption-related crime by employees of the Company	Critical	1. Sending information to management about non-compliance by employees with anti-corruption legislation, as well as liability for non-compliance with the requirements of anti-corruption legislation 2. Staff training on "Prevention of Corruption" 3. Updating of information displays "Territory without corruption" in all branches, Distribution Zones, customer service centres 4. Ensuring the implementation of the requirements of the Anti-Corruption Policy of the Company