Risk Management Strategy

All principal risk takers among the companies of the Group have a developed Risk and Capital Management Strategy. The principles and processes introduced by the Strategy seek to build, use and develop a comprehensive system of capital and risk management to ensure business continuity both in normal and stressed economic conditions, to enhance transparency of the risk and capital management processes, as well as to identify and assess significant risks in a timely manner, support capital planning and take due account of risks in the decision making process.

With a view to maintaining efficiency of the regular risk management processes:

- Group governing bodies and divisions regularly exchange information on matters connected with the recognition, identification, assessment and control of risks;
- Group governing bodies, divisions and employees have been engaged in a system of distribution of powers and responsibilities to implement key risk management principles;
- risks are regularly identified;
- responsibility for managing certain types of risks is allocated to dedicated employees;
- models are developed to quantify risks and to ensure they are comprehensively catalogued;
- measures are taken to mitigate risk factors;
- the Group's operations are tested for sensitivity against certain risk factors which are taken into account in risk assessment models;
- the Group holds regular (at least once a month) stress tests for the adequacy of equity (capital) and clearing margin, including:
  - a complex scenario-based stress analysis that takes into account simultaneous change of several risk factors;
  - back stress testing;
- management accounts are systematically drawn up and sent to Group governing bodies, including on matters connected with the recognition, identification, assessment and control of risks;
- the CCP NCC Supervisory Board Risk Committee, the Moscow Exchange Risk Committee and the NSD Management Board Risk Committee duly discharge their functions;
- the internal control system has been set up;
- financial resilience recovery plans and plans for engagement of additional resources have been developed.

Moscow Exchange has also established a separate market operator's risk management subsystem that enables it to identify and assess risks in a timely manner and to develop mitigation measures.

This system incorporates continuous monitoring of emergencies and assessment of their potential impact on the technical processes of the Exchange's markets, as well as updating the integrated operational and financial risk management system in line with adopted decisions and procedures. Further development of the risk management system is planned to reduce the vulnerability of business processes and their recovery time, to improve system redundancy based on spacing and duplication of resources, and to improve the reliability of communication systems between traders, the Exchange and depository and settlement organizations.

In addition, the Exchange has also set up a separate structural unit responsible for managing its risks as a market operator. This unit aims to identify and assess risks in a timely manner and to develop mitigation measures. The Exchange has developed and approved the Regulations on Managing the Risks of a Market Operator, which establish, in particular:

- the principles of the risk management system related to the Company's operations;
- the principles and objectives of risk management related to the activities of a market operator.

The Regulations on Managing the Risks of a Market Operator:

- classify the risks inherent to the Exchange;
- establish the procedure and timeline for an audit of the efficiency of the risk management system;
- provide basic guidance and approaches to identifying, assessing and monitoring risks;
- establish the procedure and timeline for informing the Exchange's governing bodies, executives and divisions of identified risks;
- detail a list of measures to be taken by the Exchange to ensure confidentiality of risk-related information, including confidentiality of risk reports;
- establish the frequency of stress testing, as well as the requirements for scenarios used for such testing.