APPROVED

by the resolution of the Supervisory Board
of the Moscow Exchange
on November 18, 2022 (Minutes No. 10)

RULES FOR MANAGING RISKS RELATING TO TRADE ORGANISER'S AND DIGITAL FINANCIAL ASSETS EXCHANGE OPERATOR'S ACTIVITIES

Moscow,
2022

Contents

1 Terms and definitions

Operational Risk Event Database (OREDB) means an electronic repository of information on operational risk events of the Exchange and on incidents (events) relating to operational risk, but without having any consequences and negative effects to Exchange's processes.

Risk Database (RDB) means a risk register, an electronic repository of information on non-financial risks of the Exchange.

Risk Business Owner is a sole or collegiate body of the Exchange, or the head of the business unit responsible for the processes (performed by them and/or within their competence), which are negatively affected by the operational risk and which may lead to losses or may disrupt continuity of Exchange's systems/services. The Risk Business Owner is responsible for decision-making as to respond to an operational risk event, risks, risks monitoring and controlling the implementation of control procedures within the business unit given in charge.

Exchange refers to Moscow Exchange, the Trade Organiser, Digital Financial Assets Exchange Operator.

Risk Owner is the chief of a business unit, business process or a part thereof, in the course of which the circumstances that give rise to potential operational risk, both for the Risk Owner and for the Risk Business Owner, are manifested. The company's official responsible for developing, implementing and maintaining a process and for developing control procedures.

External Operational Risk Event Database (external OREDB) refers to an electronic repository of information on external operation risk events occurred outside Moscow Exchange.

ETSH refers to external trading software and hardware tools.

Group means the Moscow Exchange Group of Companies, including Moscow Exchange, National Settlement Depository (NSD), National Clearing Centre (NCC), MICEX Finance, NAMEX, MOEX Innovations and MOEX Information Security.

Business Reputation means a qualitative estimation of Exchange's operations, as well as of activities of its shareholders and affiliated parties, by parties to civil-law transactions.

DOD refers to Duty Operations Director.

Statement on risks means a professional judgement by the risk management employees, ICS and DoICC departments exercised in a prescribed form regarding product risks – possible financial and non-financial events that may adversely affect the project product performance, reputational risks, risks of losing customer confidence.

Information Security refers to protecting against information security threats.

Information Infrastructure (IT Infrastructure) refers to a set of data processing systems and processed data used to support Exchange's operations.

Information Threats means a source of information security risk event (as a result of cyber attack).

Information System means a set of information in databases with information technology and technical means that process such information.

Key Risk Indicator (KRI) means an indicator (including statistical, financial) used to measure Exchange's performance that allows monitoring the scale and probability/possibility of risk realisation.

Compliance Risk means a risk of losses as a result of non-compliance with legal requirements, internal documents, self-regulatory organisation standards (if such rules and standards mandatory applicable) and as a result of sanctions and (or) other interventions taken by the oversight bodies. We use the term 'regulatory risk' to describe compliance risks, since it is one of (but not the only one) Exchange compliance risk components.

Control Procedures means a set of measures aimed at reducing the probability /possibility of the emergence of risk, minimising the potential damage from risk occurrence and controlling the consequences of a risk event.

Conflict of Interest refers to a situation where an indirect or direct personal interest, actual or potential benefit of an Employee, an Affiliated Party of the Exchange affects or

may affect fair and effective performance of their duties and may have an adverse effect on the Exchange, its clients and business partners.

Credit Risk means risk of a loss resulting from a contractor's failure to meet contractual obligations, whether partially or in full.

Risk Mitigation means risk minimisation, so that the activity continues in a modified form, in particular, by introducing new or optimising existing control procedures.

Abnormal Situation means circumstances that cause and/or create preconditions for the emergence of failures (outages) during the operation of hardware and software subsystems of the Exchange in the course of operation and/or directly impeding normal (routine) functioning, as well as other circumstances, which:

- have caused or may cause violation of the procedure of interaction between Moscow Exchange and other Moscow Exchange Group members, the Bank of Russia, VEB.RF, the Pension Fund of the Russian Federation, and the Federal Treasury on any of the markets;
- have led or may lead to a violation of the procedure and timing of operations, procedure of access of participant or group of participants to trading, as well as disclosure and provision of information as prescribed by internal documents of the Exchange for the relevant market.

Non-financial risks refer to operational risk (including information security and business continuity risks), reputational risk, strategic risk, project risk and legal risk, compliance risk, including regulatory risk.

Informatization Object means a set of access objects and resources, information processing tools and systems, including automated systems used to support informatization of the Exchange’s business and/or technological processes, used in order to provide financial services

Information System Operator refers to an individual or a legal entity operating information systems, including processing of data residing in their databases.

Operational Reliability refers to the ability to ensure continuous operation of critical processes while observing operational reliability targets.

Operational Risk means any risk exposure consequences leading to suspension or termination of Exchange's services, whether to full extent or in part, and risk of expenses (losses) for the Exchange from failures and (or) faults in Exchange's software and hardware, inclusive of software and hardware, information and communications facilities used to facilitate trading and (or) used in Exchange's internal business processes, as well as from errors of employees and (or) external exposure affecting the Exchange.

Plan Coordinator means an employee responsible for coordinating risk minimisation/closure activities.

Risk Avoidance (Risk Aversion) means refusal to accept/transfer certain types of risk entailing the refusal to perform any of operations and provide any services with inherent risk. Since these actions can lead to a decrease in the Exchange's revenues, the decision to avoid/retain risk should be made with account for risk and revenue amounts.

Risk Transfer means that the activity continues, and changes are made to it, as a result of which the risk is fully or partially transferred to a third party.

Business Continuity & Recovery Plan (hereinafter, BC&R Plan) refers to an internal document of the Exchange, which defines objectives, targets, procedure, methods and timing to implement a set of measures on prevention or timely elimination of consequences from possible violation of everyday operations of the Exchange (business units of the Exchange) caused by unforeseen circumstances (occurrence of emergency situation or other event that is likely to happen, but hardly to predict and relates to a threat of significant financial losses or other consequences preventing the Exchange from fulfilling assumed obligations).

Legal Risk refers to the risk of losses resulting from inefficient organisation of legal work, leading to legal errors in the Exchange's activities due to actions of employees or governing bodies; breaches of contract terms by the Exchange and the Exchange's customers and counterparties; contract provisions that do not meet the Exchange's rights and interests;

imperfect legal system; Exchange, its customers and counterparties coming under different jurisdiction.

Risk Limit (Risk Appetite) means a maximum quantum of risk that the Exchange is ready to accept in pursuit of its strategic objectives.

Risk Acceptance means that the activity, which this type of risk is associated with, continues unchanged. If the risk is accepted, the need to establish a monitoring system for various indicators characterising the level of the risk shall be considered. The risk acceptance procedure is consolidated in the Exchange's internal documents. The procedure for accepting operational risk in excess of the established risk appetite in some cases should be accompanied by a reasoned judgement on the adequacy of funds to cover losses from the events caused by such risk, calculated on the basis of historical data for previous years (at least 10 years) in the presence of data and a model for conducting calculations.

Project refers to time-limited activities to create new (unique) products, services or outcomes of value to the Moscow Exchange Group and third parties.

TC S&H refers to software and hardware suite of the Exchange's Technical Centre.

Risk means an event or a condition that, if occurs, has a negative impact on business processes, services, and customers, and also leads or may lead to potential losses in a form of lost revenue, additional expenses or a negative impact on business reputation.

Risk Appetite means the maximum amount of risk that the Exchange is ready to accept at given time interval in order to achieve strategic goals. Risk appetite is articulated as a system of quantitative and qualitative benchmarks that limit the level of risk accepted.

Risk Manager refers to an employee of the business unit responsible for the organisation of the risk management system (DoORIS&BC);

Product Risk means potential financial and non-financial events that may have an adverse impact on the economic performance of the project product, reputational risks, risks of losing customer confidence. These are recorded in the consolidated Statement on product risks generated by the risk management business units.

Regulatory Risk means the risk arising for Moscow Exchange from expenses (losses) and (or) other unfavourable consequences as a result of non-compliance of its activities under the license of the exchange for trade organiser's activities, activities of the digital financial assets exchange operator carried out pursuant to Moscow Exchange's inclusion in the registry of digital financial assets exchange operators, activities under financial platform operator's license to operate pursuant to inclusion in the registry of financial platform operators with the Russian legislation regulating operations of Moscow Exchange, trading rules, rules of digital financial assets exchange, financial platform operator's rules, constituent and other internal documents of Moscow Exchange, and (or) as a result of measures imposed by the supervisory authorities towards Moscow Exchange.

Information Security Risk refers to the risk of possibility Exchange's information assets losing their information security properties (confidentiality, integrity, accessibility) due to implemented information security threats. Possible information security risk implications include:

- occurrence of Exchange's losses and those of its clients and counterparties;
- interruption of Exchange's financial and (or) information services continuity when information threats are materialising.
- Exchange's failure to protect its clients' interests when they incur losses due to materialised information threats;
- failure to comply with the requirements of the legislation of the Russian Federation in the field of information protection, etc.

Reputational Risk means a risk of consequences involving expenses (losses) for the Exchange as a result of negative perception of the Exchange by its counterparties, trading members and their clients, shareholders of the Exchange, the Bank of Russia and other legal entities or individuals who may adversely affect Exchange's ability to maintain existing and/or to establish new business relations and continuously maintain access to sources of funding (hereinafter referred to as RR).

Project Risk means a possible event or condition which may adversely affect the project parameters, such as the project term, content, budget/financing limit.

Information Security Threat Risk refers to possibility of materialisation of information security threats (with consequences thereof), which are caused by deficiencies in operational reliability and information protection processes, including technological and other measures, deficiencies in the application software of automated systems and applications, as well as inconsistencies in the specified processes with Moscow Exchange's activities.

Information protection system means the aggregate of information protection measures which are applied directly in order to ensure information protection, implementation of the above information protection measures processes, resource and organizational support required for the implementation of such information protection measures.

Risk Event refers to an event, situation or a circumstance in which risk is realised (manifested) and which may cause the Exchange to incur losses (expenses), as understood by the Rules, events of non-financial risks, i.e. operational, reputational, strategic and regulatory (compliance), legal and project risk events.

Operational Risk Event (ORE) refers to an event, a situation, or a set of circumstances that are characterised by the realisation (manifestation) of operational risk and could lead to losses[1].

The Total Risk Limit is a maximum potential loss that the Exchange may incur as a result of risk occurrence within its risk appetite.

PNS refers to Prompt Notification System.

Strategic Risk means a risk of expenses (losses) for the Exchange resulting from wring decisions in the process of management, including in developing, approving and executing documents that determine development directions for the Exchange, inadequate implementation of decisions made in the process of management, and ignoring the changes in external factors that affect or may affect Exchange's management process.

[1]An operational risk event also refers to an event of information threat risk (including cyber risk and other types of information threat risks) if the event has led to a business process disruption.

Non-financial risk stress testing refers to simulating various negative scenarios of non-financial risks with financial and non-financial implications for the Exchange. One of the operational risk stress scenarios is load testing, i.e. assessment of resistance of software and hardware used in organising trades to significant changes: exceptional, but believable events related to the violation of business processes and the external environment.

Non-financial risk scenario analysis (scenario analysis) is a specially structured forecast of losses and operational and (or) other non-financial risk events such losses arise from, based on expertise in the area where the risks are to be assessed. Scenario analysis involves predicting the occurrence of an operational risk event, the likelihood of its occurrence, and an estimate of the amount of potential loss within the scenario under analysis. Scenario analysis can be based on collected data on internal and external operational risk events, on expert judgement, on findings from quantitative and qualitative analysis, and on the results of risk self-assessment and control procedures, ongoing operational controls, values of key risk indicators, internal and external audits and audits by external supervisory bodies.

TCS refers to Trading & Clearing Systems of the Exchange.

Information Security Threat means a threat of violation of information security properties (availability, integrity, or confidentiality) of information assets of the Exchange.

Risk Factor means a circumstance that caused or is capable of causing the occurrence of a risk event.

Normal Functioning Disruption Factor means a situation that may pose a threat of interruption of normal activities. Examples:

- disruption of normal functioning of automated systems supporting critical processes of the Exchange;
- failure (inaccessibility) of key communication channels including corporate network of the Exchange, the Internet information and telecommunication network, and other channels of communication with interacting organisations, which are necessary to maintain critical processes of the Exchange;

- physical absence of Exchange employees at their workplaces due to fire, floods, accidents, acts of terrorism, subversion, sabotage, natural disasters and other force majeure;
- other cases that may affect normal operation of the Exchange.

Target Level of Risk means the level of risk that the Exchange is seeking to achieve when planning its risk management measures.

Digital Financial Asset refers to digital financial assets issued and recorded in the Information System[2].

Emergency Situation (ES) means external actions that might impair continuity of Exchange's operations and ability of the Exchange to fulfil its obligations, subsequently leading to potential losses for the Exchange. Provided that external influence is understood as a specific situation in a certain territory, which has developed as a result of an accident, a dangerous natural phenomenon, a catastrophe, an outbreak of the disease posing threat to others, a natural or other disaster that may or has entailed human casualties, damage to human health or the environment, significant material losses and disruption of the living conditions.

The following are possible emergencies: large-scale non-standard and emergency situations comparable in duration and effect, potential tangible losses and negative non-tangible consequences to a municipal, inter-municipal, regional or inter-regional emergency resulting in factors interrupting normal operations of the Exchange.

Expert means an employee of the business unit involved in the self-assessment, the owner of the processes subject to the self-assessment.

DoICC means the Department of Internal Control and Compliance.

DoC means the Department of Communications.

CSD means the Customer Support Department.

[2] In this paragraph the Information System refers to a distributed ledger, i.e. a set of data bases used for issuing and circulating digital financial assets and operated by the National Settlement Depository.The identity of information residing in such data bases is ensured through establishes algorithms (algorithm).

DOD refers to the Duty Operations Director. An employee that organises and coordinates the work of emergency response centres.

DoORIS&BC means the Department of Operational Risks, Information Security and Business Continuity. It belongs to risk-management business units.

ST means the Strategy Department.

DoT&SSM means the Department of Trading and Support System Management.

Project and Product Committee (PPC) refers to an advisory body at the Executive Board. The Committee performs the following tasks:

- create a unified approach to managing group-wide projects (this including control of projects in the project portfolio, development of recommendation on strategic decisions on projects and project programmes, etc.);
- improve the quality of project and product development through their in-depth study, including by the Committee's risk management experts;
- ensure interaction across the Moscow Exchange Group companies when taking decisions on projects and products by including the representatives of the Group as members of the Committee.

OD refers to the Operations Department.

PO refers to the Project Office.

IAS refers to the Internal Audit Service.

ICS refers to the Internal Control Service.

FRMO refers to the Financial Risk Management Office. It belongs to risk-management business units.

LD means the Legal Department.

DR Test (Disaster Recovery Test) means testing of software and hardware and network communications of the Moscow Exchange Group located in the main and backup data processing centres.

NIST means the National Institute of Standards and Technology (SP 800-30 Guide for Conducting Risk Assessments).

NPV means Net Present Value.

OSSTMM means the Open-Source Security Testing Methodology Manual.

OWASP means the Open Web Application Security Project.

PTES means the Penetration Testing Execution Standard.

TCO means the Total Cost of Ownership.

Terms not specifically defined in the Rules are used in the meanings defined in the internal documents of the Exchange, laws and other regulatory documents of the Russian Federation.

2 General provisions defining the risk management objectives

2.1. These Rules for Managing Risks

Relating to Trade Organiser's and Digital Financial Assets Exchange Operator's Activities (hereinafter, the Rules) shall be a guideline document to define key principles for creating a risk management system in Moscow Exchange (hereinafter, the Exchange,) as related to trade organisation, exchange of digital financial assets (DFAs) and transactions with own holdings (hereinafter jointly referred to as the risks of the Exchange), and to form a regulatory framework for the effective risk management system appropriate to the scale of Exchange's operations.

2.2. The Rules are based on the following requirements:

- Federal Law of the Russian Federation of 21 November 2011 No. 325-FZ 'On Organised Trading' (hereinafter, the Law on Organised Trading);

- Federal Law of 31 July 2020 No. 259-FZ 'On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation'.
- Bank of Russia Regulation No. 437-P dated 17.10.2014 'On Organised Trade Activity';
- Regulation No. 779-P of 15 November 2021 'On setting mandatory requirements for non-credit financial institutions regarding operational reliability when carrying out activities specified in Part I of Article 76.1 of Federal Law No. 86-FZ of 10 July 2002 'On the Central Bank of the Russian Federation' to ensure continuity of financial services (except banking services)';
- Bank of Russia Ordinance No. 4791-U, dated 7 May 2018, 'On the Requirements for Trade Organisers to Create a System for Managing Risks Related to Trading and Transactions with Their Assets and on the Requirements for Trade Organisers' Documents Stipulating Measures to Mitigate the Said Risks and Prevent Conflict of Interest';
- Bank of Russia Ordinance No. 4792-U, dated 7 May 2018, 'On the Requirements for the Procedure for Trade Organisers to Exercise Internal Control and Internal Audit' etc.
- GOST R 57580.1-2017 'Financial (Bank) Transaction Security. Data Protection in Financial Organisations. Core Arrangements and Controls' national standard of the Russian Federation.

2.3. Risk Management purpose.

The purpose of Exchange's risk management shall be to limit the risks assumed in all activities of the Exchange in accordance with company's strategic goals and objectives; ensure the adequacy of capital to cover the risks assumed and to ensure reliable business processes.

The risk management objectives are achieved through a comprehensive system approach entailing the following tasks to be dealt with:

- identification, analysis, monitoring, control and mitigation of risks (or their acceptance/avoidance) on an ongoing basis;
- information sharing between structural units of the Exchange while identifying risks;
- qualitative and quantitative assessment (measurement) of risks;
- establishing a procedure for risk management reporting to corporate bodies of the Exchange;
- establishing a system of control measures for the prevention of risk events, maintaining an acceptable level of risk (risks), as well as a system of a rapid and adequate response to eliminate the consequences of such events when they occur;
- distribution of risk management authority and responsibility between business units and employees.

2.4. The Exchange has created a separate business unit responsible for organising the risk management system, the Department of Operational Risks, Information Security and Business Continuity (hereinafter referred to as DoORIS&BC), which is managed by the Director of DoORIS&BC.

3 Risk consequences materiality qualifiers for the Exchange to qualify such risks (excluding operational risks of the Exchange) significant, and the procedure for comparing the results of identified risk assessment against these qualifiers

A risk can be recognised as significant if the adverse impact of the risk has a material (significant) impact on one or more indicators below:

- P&L;
- reputation;
- compliance;
- info security.

Significant risks, in any case, will be those that are recognised as significant in accordance with the requirements of Bank of Russia Ordinance No. 4791-U.

In qualifying such risks significant, Moscow Exchange defines the following materiality qualifiers for the risk consequences:

- non-compliance with requirements of the Russian Federation legislation which implies penalties (fines) imposed by the supervisory authorities exceeding RUB 700,000 per year;
- possible suspension of certain operations, suspension of activity;
- surge of negative feedback from customers/counterparties, which is 70% up of average negative publications from the previous year;
- negative publicity about the leadership team of the Exchange;
- financial loss exceeding the limit set for the given risk type for the current year;
- functional failure of Exchange's key systems;
- 12-month or longer delay in key strategic directions' implementation;
- considerable increase in the cost of key strategic directions;
- substantially lower returns from strategic directions implementation;
- substantially lower returns on Exchange's key products;
- massive leaks of data, successful attacks on Exchange's key systems;
- other consequences that may have a strong negative effect on Exchange's operations.

The Exchange shall compare the results of risk assessment against the above materiality qualifiers as follows:

- implement activities aimed at identifying risks throughout a calendar year;
- assess risk factors and potential consequences of the risks identified;
- model the possible and likely outcomes of the risks identified;
- analyse and measure potential effects of the risks identified;
- match the results against risk consequences materiality qualifiers set out herein.

- If the findings of identified risks assessment demonstrate compliance with materiality qualifiers for consequences, then a decision is made to recognise these risks as significant.

4 The Risk Limit (Acceptable Risk) and Total Risk Limit Methodology of the Exchange

The Exchange applies the following approaches to determine risk limits and total risk limits:

4.1. Estimate risk implementation on the basis of historical data, and establishing the limit values at the level of several previous years' average values. Estimate risk implementation on the basis of historical data depends on a series of annual parameters continuously taken in a definite period, and a period of 10 years is used as such.

4.2. Perform scenario analysis on the most likely risk scenarios and set metrics at the level of resulting values.

4.3. assess potential loss impact on the Exchange's financial performance and establish caps based on the size of the potential loss where there is no impact on the Exchange's strategic initiatives;

4.4. Perform risk stress-testing to identify limits of expected losses from risk occurrence.

4.5. To identify total risk limit an approach is used that applies realistic scenarios for estimating losses from of one or more than one of the identified risks occurred together. However, risk occurrence must not destabilise the Exchange's financial position.

The Supervisory Board of the Exchange sets risk limits per each calendar year.

5 Procedure for identification of risk limitation breaches

To identify risk limitation breaches, compliance with the set quantitative and qualitative risk appetite metrics is monitored. Risk appetite metrics are calculated monthly by the business units responsible for managing individual risk types and are consolidated by DoORIS&BC. The procedure for identifying breaches of risk limitation is as follows:

- An employee of the business unit responsible for risk management analyses risks upon their detection, assesses the level of risk, checks for threshold breaches, the reasons for and consequences from such breaches.
- Should any violations of the set risk limitations be identified, the employee initiates the development of plans and actions to mitigate negative consequences jointly with departments responsible, and to reduce or avoid the risk, or to revise risk limitations set;
- If the set limits (thresholds) of the risk appetite are exceeded, the information is brought before the Supervisory Board of the Exchange.

Findings from risk appetite monitoring result in a report, which is submitted by the Director of DoORIS&BC to the Executive Board on a monthly basis and to the Risk Management

Committee of the Supervisory Board on a quarterly basis. Reports contain information on risk appetite metrics, the level of risk at the reporting date, information on identified breaches of risk limitations and measures to address such breaches and reduce the level of risk (if necessary).

If a risk effecting risk appetite threshold values occurs, decisions shall be made as to the measures required to mitigate individual risks affecting the level of Exchange's risks.

6 The procedure for implementing corrective measures on the identified breaches of Exchange's risk limitation and/or other risk mitigation or risk avoidance measures

When a breach of risk limitations is identified, or in the course of risk mitigation or avoidance, the staff of the business unit responsible for risk management shall follow the following procedure:

6.1. determine the cause of breaching the risk limitation or detect factors that may contribute to occurrence of the identified risk;

6.2. identify the possible consequences that may arise from such a risk;

6.3. Define employees of the Exchange responsible in the area of risk factors and risk consequences;

6.4. develop jointly with persons named above a range of activities aimed at eliminating the risk factors, or activities aimed at minimising the severity of risk consequences, or activities aimed at risk avoidance;

6.5. Agree on responsible employees and deadlines for the named activities with the heads of Exchange business units;

6.6. regularly monitor the deadlines and execution of assigned activities;

6.7. produce reports on the status of activities for Exchange's collegial corporate bodies.

7 Procedures to implement processes and measures to identify, analyse and monitor risk, share information across business units and corporate bodies of the Exchange, as well as processes and measures carried out by the Exchange in managing certain types of risks

7.1. Identification of Exchange's risks.

Risk identification procedure:

- Each employee of the Exchange shall inform DoORIS&BC of risks as soon as they are identified.
- DoORIS&BC collects information on risks (both internal and external) that may cause damage to the Exchange, risk factors, possibility/likelihood of risk occurring in the course of Exchange's activity, the extent of damage (expected, worst case, most frequent, etc.);
- DoORIS&BC may engage FRMO, LD, ICS, DoICC and other teams to identify the types of risk;
- DoORIS&BC performs a self-assessment of operational risk. Self-assessment shall be in the form of interviews or survey among responsible business units performed on the regular basis, but at least once a year.
- DoORIS&BC performs diagnostics on business processes, analyses overlaps in the competences and responsibilities of business units and employees of the Exchange;
- Various business units analyse the outcomes of internal and external audits performed on controls/procedures/systems;
- Risk management business units analyse new products, processes and systems, project and non-project tasks (perform analysis of all innovations implemented by the Exchange: changes in structures and procedures, launch of new services and technologies, development of new lines of business, etc.).

- Risk Management analyses the risks of new strategies and changes to existing ones.

7.2. Analysis and assessment of Exchange's risks;

The following methods are used for risk analysis and assessment, inter alia:

- Scenario analysis that includes identification of threats that according to the Trade Organiser's opinion may lead to a failure of trading tools to work, monitoring of the current status of trading tools, in particular with respect to the need to update them;
- Processing of statistical and analytical RDB and extremal OREDB data which is used to assess the impact of Exchange's risks on its financial soundness is assessed through estimating risk events which, also given probability and level of such risks, will lead to losses;
- Stress-testing of software and hardware facilities used for trade organiser's and digital financial assets exchange operator's activities is also run to detect (identify), analyse and assess operational risks. Stress-testing frequency is determined by Exchange's internal documents, but it shall be performed at least once every six months.

Assessment procedures:

- identification of risk factors and sources, identification of types of risk;
- analysis of information on risks (both internal and external) that may cause damage to the Exchange, possibility/likelihood of risk occurring in the course of Exchange's activity, the extent of damage/loss(es) (expected, worst case, most frequent, etc.);
- matching the results of identified risks assessment against the set materiality criteria in accordance with Clause 3 of these Rules;
- setting risk limits and total risk limits in accordance with Clause 4 of these Rules;
- analysis of information on the applied controls based on the expert opinion of Exchange's business units within the scope of their functions and tasks;
- A product risk assessment is performed at project opening in all next phases of the project life cycle. A product risk assessment is a mandatory part of any project launch and is performed on non-financial and financial risks for all projects. It includes:

    - description of effects from the future product on Exchanges resistance to risk to the extent of full list of financial and non-financial risks;
    - non-financial risk assessment and a risk valuation for the future product;
    - assessment of risk effects on Exchange's activity;
    - assessment of potential losses by risk types inherent in the product;

- assessment of the product's return given the risks accepted in relation to income-generating projects. This assessment results in a Statement on Product Risks, which is taken into account by the Executive Board when making decisions on the project product.

7.3. Exchange’s risk monitoring, control and mitigation, or risk avoidance.

Monitoring is a system of activities aimed at the periodic collection and analysis of information on the change of risk level.

Exchange’s risk monitoring procedures includes:

- tracking changes in the level of risk across Exchange's business units;
- prompt response to changing risk level across Exchange's business units in order to reduce the level of risk;
- timely response actions taken to reduce risk to an acceptable level.

The Exchange shall, as part of its monitoring, control and risk mitigation or avoidance efforts, perform the following activities:

- determine the level of risk, also whether it meets the risk exposure limit set by the Exchange;
- develop and implement measures to correct identified breaches of risk limits and measures to reduce or avoid risks. For significant risks, the Exchange develops internal documents containing an action plan to mitigate or avoid such risks. These actions and updates on their implementation are reported to authorised governing bodies of the Exchange on a regular basis:
  - actions regarding project, product and strategy risks are reported to the Executive Board;
  - measures to mitigate risk-appetite non-observance risks are reported to the Executive Board of the Moscow Exchange, the Risk Management Committee at the Supervisory Board and to the Supervisory Board;
  - actions regarding material risk events are reported to the sole executive body of the Moscow Exchange, Executive Board and the Risk Management Committee at

the Supervisory Board and may be reported to the Supervisory Board at the discretion of the Chairman of the Risk Management Committee;

To monitor risks, the Exchange introduces key risk indicators as the indicators of Exchange's activity (including statistical and financial indicators), which are used to record operational and other types of risk events, thresholds for these indicators are set, against which the probability of the recurrence of these events is assessed.

Key risk indicators (hereinafter, KRI) include:

- frequency and level of impact indicators for operational and other types of risk events that occurred during a reporting period;
- indicators that allow monitoring the effectiveness of control procedures in business processes and assessing the associated risks;
- indicators that measure the scope of a particular area of Exchange's business or a particular business process, in order to determine the level/degree of their exposure to risk.

For each KRI thresholds are defined, i.e. numerical values showing the maximum allowable values for an indicator. Any deviation from these thresholds may indicate higher probability of a risk event, indicating the need to take organisational control measures and/or measures to minimise risk occurrence probability. Risk monitoring procedures with KRI include the following:

- development of a KRI register (including description, responsible persons, and frequency of monitoring);
- setting thresholds in a KRI register;
- KRI data collection for the reporting period and analysis of the values obtained;
- generation of a report to governing bodies of the Exchange with proposals on action points based on the current KRI values (if necessary);
- tracking implementation of risk mitigation activities (if necessary);
- KRI register review on a periodic basis.

DoORIS&BC and risk management business units control risks through implementing the following measures:

- the overall level of risk and the timeliness of response measures from responsible persons are controlled on a daily basis by way of monitoring;
- DoORIS&BC annually monitors measures implemented under identified and/or occurred operational risks;
- ICS regularly performs subject-matter checks;
- FRMO controls treasury limits and other financial risk metrics, provides pre-approvals and pre-checks in accepting clients, concluding agreements with counterparties, admitting securities to trading, launching new products/services, and in some other cases;
- DoICC gets preliminary approvals and checks when accepting clients, concluding agreements with counterparties, admitting securities to trading, launching new products/services and in some other cases, organises automated controls, those including for checking persons against compliance lists, ensures policies and procedures are in place and provides mandatory training;
- LD carries out comprehensive analysis of legal risk causes of occurrence, as well as provides prevention of occurrence of legal risk events, risk factors occurrence implications.
- DoC investigates and analyses the Trade Organiser's performance indicators; monitors complaints and claims made against the company, including those related to customer service and counterparties' quality, compliance with good business practices; as well as positive and negative reviews and feedback concerning the shareholders and affiliates, in mass media.
- Strategy Department develops draft amendments to on-exchange trading implementation procedure or the activities related to on-exchange trading implementation, providing of additional services, admission of new financial instruments to on-exchange trading, as well as other organizational and/or technological changes;
- analyses feasibility of introducing draft amendments;
- The Exchange's corporate strategy is assessed to find out whether it is feasible and expedient to implement, and if the Exchange so decides, the corporate strategy is amended.
- Project Office provides for analysis of possible events or conditions occurrence of which may adversely affect the project's parameters (such as the project's

timeframe, content, budget/funding limit), develops measures to prevent risk implications.

- Independent monitoring regarding risk management measures implementation is performed by IAS at least once every three years and (or) off-schedule, as well as by external auditors and regulating authorities.

Risk mitigation efforts include the following measures:

- insurance;
- automated control procedures and processes;
- exercise authority control as part of information security risk management;
- four-eye principle;
- regulated internal processes;
- limits and their monitoring;
- data back-up;
- staff training and incentive programmes.

Risk avoidance for the Exchange means that the Exchange avoids undertaking a particular risk-generating activity and/or a project.

The Exchange may accept risks, i.e. to perform activities in some business areas without minimising and (or) avoiding risk. A decision to accept risks is taken by the authorised corporate body of the Exchange and (or) by the heads of business units within their authority.

The financial risk measures in these areas are outlined in the Financial Risk Policy.

7.4. Procedure for sharing information on risks between business units of the Exchange, between business units and corporate bodies of the Exchange.

Procedure for sharing information on risks between business units of the Exchange and corporate bodies of the Exchange is performed through regular and unplanned (ad-hoc) risk reporting.

The Exchange has established the following procedure for the Exchange employees to provide risk management information:

Working groups meet at least once a month with regard to risk event analysis, risk level assessment and the status of risk mitigation measures. The meeting procedure is as follows:

- An employee of DoORIS&BC at least once a month meets with employees and heads of structural units engaged in implementing risk minimisation measures;
- Operational risk events that occurred during a reporting month are analysed and discussed;
- Status of action points implementation regarding events identified in previous periods are analysed.
- DoORIS&BC submits a report on the results of load testing to responsible IT business units no later than 10 days from the date of the report.

Unless otherwise stipulated in the internal documents of the Exchange:

- frequency for notifying employees and reporting risks to business units of the Exchange are determined by DoORIS&BC Director based on his/her professional judgement generated with regard to the risk assessment, the Exchange's needs, amount of risk and the principle of materiality;

- frequency and the form for employees of the Exchange to provide information are determined according to requests of DoORIS&BC Director.

7.5. Taking measures aimed at preventing overlapping (part overlapping) of competences of Exchange’s business units.

These measures include those listed in the Procedure for the Exchange to take measures to prevent and manage conflicts of interest arising for the Exchange in connection with combining its activities with other activities, as well as the analysis of business processes by DoORIS&BC as part of a risk self-assessment process.

7.6. Determining the list of software and hardware tools of the Exchange that require protection against illegal actions, whose failures and/or errors may result in the partial or complete suspension or termination of organised trading services and/or have another negative impact on operations of the Exchange.

The procedure for defining the list includes the following activities:

1) The list of Exchange’s hardware and software is compiled based on the criticality of the systems and recovery time required in the event of failure and/or error;
2) All of Exchange's software and hardware tools are grouped by requirements to their reliability;
3) Reliability groups include the following:
    - Group A – critical:
        - 1A – trading and other systems as real-time systems;
        - 2A – main data processing systems;
        - 3A – other critical data processing systems with lower recovery time requirements.
    - Group B – important;
    - Group C – non-critical (office systems, software development systems, gaming and training systems etc.).
4) Data processing systems (the system constituent tasks) are grouped by reliability according to a methodology based on business process analysis and approved by the Architecture Committee. A system (its constituent task) which, for whatever reason, is not assigned to a reliability group by default, is assigned to Group C.
5) Determining the properties of the reliability group, which include:
    - accessibility coefficients for applications within a group;
    - isolation and instrumentation requirements for the environments in the application group;
    - recovery time factors for the application systems within the group, as determined by the business continuity programme, namely:
        - target recovery time;
        - acceptable data loss bands.
6) Accessibility coefficients are set for each of the groups of systems. To ensure the high availability of its functional systems, the Exchange implements backing up at all levels of the structural hierarchy, from physical components, servers, networks and storage systems to backing up at the level of the application software, network infrastructure and the Exchange’s data centre system.

7.7. Listing and implementing information security measures.

Operational risk associated with a breach of information security is inherent in Exchange's operations. This is a fact of life, and the risk can be reduced only to a certain residual level. To manage the operational risk associated with the security of information, the Exchange ensures:

- identification and accounting of objects of informatisation;
- application at various levels of the information infrastructure, selected by the Exchange and information protection measures aimed at directly ensuring the protection of information;
- application of information protection measures selected by the Exchange, which ensure the completeness and quality of information protection that are acceptable for the Exchange, included in the information security organisation and management system;
- application of information protection measures selected by the Exchange aimed at ensuring the protection of information at all stages of the life cycle of automated systems;
- assessment of the residual level of operational risk caused by incomplete or poor-quality selection and application of information protection measures, and processing of this risk;

The above measures are implemented by the Exchange to ensure confidentiality and protection of information on Exchange's risks and information provided by the Exchange to the service provider.

Reducing the operational risk associated with a breach of information security is ensured by making appropriate choices, improving the completeness and quality of the application of appropriate information security measures. Completeness and high quality of implementation of information protection measures are achieved by planning, realisation, inspection and improvement of information security risk management processes, as well as by implementation of information protection measures during the life cycle of automated systems and applications.

Residual operational risk connected to incomplete or poor-quality implementation of information protection measures included in the information protection system is assessed in accordance with a procedure defined by the legal requirements, on the basis of assessing compliance of the Exchange's information protection system to 'Financial (Bank) Transaction

Security. Data Protection in Financial Organisations. Core Arrangements and Controls' national standard of the Russian Federation.

Procedure for listing and implementing information security measures in compliance with legislation requirements includes the following activities:

- DoORIS&BC in association with the responsible business units develops and approves internal documents that outline control measures to ensure information security efforts;
- DoORIS&BC in association with the responsible business units implements information security measures and implements control measures to ensure that information security tools are in place.

  Information security measures include the following:
- raising personnel involvement and awareness of the Exchange in identifying breaches of information security requirements and countering information threats;
- information security in access and registration control;
- information security throughout the life cycle of automated systems;
- information security with antivirus solutions;
- information security when using the Internet, network security in overall;
- control of IT infrastructure integrity and safety;
- data leak prevention;
- security and control procedures (cryptography, encryption, protection against unauthorised access during information transmission or storage, software restricting access to data, authentication and authorisation of participants and users), also when working distantly;
- information security when assigning and allocating roles;
- regulating and documenting information security activities, those including procedures to register and sore information;
- detection and response to information security incidents, those including critical architecture incidents;
- monitoring and analysing information security measures, analysis of causes and consequences of incidents;

- timely improvements on information security tools, use of data on relevant information security threat scenarios in order to ensure operational reliability of the Exchange;
- ensuring long-term planning of information and computer systems, their requirements specification, selection of suppliers and control of system and data processing and transmission technology projects for the Exchange;
- arrangement of interactions between the Exchange and stakeholders, including Exchange's clients, for the purposes of exchanging information on relevant scenarios of realisation of information security threats;
- ensuring that employees have access only to information necessary for them to perform their official duties to the extent of the authority granted;
- restricting access through the use of software features;
- existence of access control systems for different levels of databases and operating environment at LAN level;
- ensuring procedures for a continuous operation of the Exchange's software and hardware tools used to perform trade organising activities, and procedures for resuming business and technological processes and operation of informatisation objects after incidents, including:
  - existence of a fully backed-up computer system architecture with no non-redundant points of failure and resilience to multiple hardware failures of any type of component capable of supporting the main electronic systems used by the Exchange;
  - availability of alternate communication channels;
  - having a relevant action plan in place to deal with the need for reserve capacities and components of the data centre and to regularly practise actions listed in the plan;
  - procedures to recover internal processes and systems that have been disrupted and return to normal operation;
  - existence of solutions that are built into the application systems and ensure load balancing and mutual backing up at the gateway level and at the level of the main data processing servers;
  - using high availability clusters with built-in backing up of main components as the platform for the most critical tasks;

- using telecommunication devices with a standard back up of primary units;
- using fully backed-up architecture storage devices for storing databases and other critical information;
- regular (at least once a day) back-up procedures for all critical data are in place and strictly followed, with back-up copies to be kept and regularly updated;
- regulated recovery procedures in place;
- the availability of back-up multi-purpose workstations;
- the computer centre has an automatic fire extinguishing system;
- 24/7 monitoring of computing and telecommunication resources, the Exchange's computer centre premises;
- reallocation of roles, authorities and responsibilities of business units and employees;
- measures to maintain adequate information support, assessing the preparedness of external information service providers to respond to emergencies.

- arrangement of interactions between Exchange's business units, between the Exchange and the Bank of Russia, stakeholders when responding to incidents and resuming business and technological processes and operation of informatisation objects after incidents.

The information security risk management policy identification measures used by the Exchange ensure:

- identification of the structure and set-up of the information security risk management system, as well as allocation of functions, roles and responsibilities as part of managing information security risk;
- management of information security risk;
- participation of the Supervisory Board and executive bodies of the Exchange in handling of information security risk management.

Information security risk assessment measures apples by the Exchange ensure:

- identification of the critical architecture;

- identification of information security risk;
- information security threat detection and modelling;
- assessment of information security risk.

Measures aimed at elaboration of activities minimizing the negative impact of information security risk and used by the Exchange ensure:

- selection and implementation of information security risk response method;
- elaboration of activities minimizing the likelihood of realisation of information security risk;
- elaboration of activities limiting the severity of consequences of realisation of information security risk.

Measures aimed at protection against realisation of information security risk and used by the Exchange ensure:

- protection of Exchange's information;
- operational reliability;
- management of the risk of realisation of information security risk when interacting with service providers;
- management of internal perpetrator risk;
- management of information security risk in a financial ecosystem.

Measures aimed at arrangement of resourcing (personnel and financial) and used by the Exchange ensure:

- arrangement of resourcing (personnel and financial) for processes of the information security risk management system;
- arrangement of resourcing (personnel and financial) for operation of DoORIS&BC.

In case of any registered emergencies (faults or significant reduction of functionality of information infrastructure components) in the information infrastructure that cause temporary technical inability to implement all information protection measures included in the information protection system, the Exchange provides for taking by its employees of

actions aimed at performance of their official duties in the context of absence of several information protection measures, as well as proper control of such actions.

Information protection measures included in the information protection system are implemented, inter alia, to protect:

- backup copies of access resources, databases and information archives;
- information processed by virtual machines, as well as when implementing the virtualization technology.

When storing and processing information and documents related to organisation of trading, a user access control system is in place on workstations and servers to allow access to data only by authorised employees and to prevent unauthorised access by all other employees and unauthorised persons. This system operates both at the system and network level and in the applications used by the Exchange.

The Exchange has defined, implemented, recorded and monitored rules and procedures in place for monitoring access to information, analysing and storing data on employees' actions and transactions in order to implement efforts according to the data protection process in identity and access management described in GOST R 57580.1-2017.

The Exchange maintains logs of activities and operations on automated workstations, server and network equipment, and firewalls for their use in responding to information and document incidents.

Procedures for monitoring information and analysing data on actions and transactions apply set criteria to identify unlawful or suspicious actions and transactions. These monitoring and analysis procedures are applied on a regular basis to all actions and transactions executed.

7.8. Control of software and hardware access permissions for Exchange's employees.

Procedures to control software and hardware access permissions for Exchange's employees:

- User permissions to access the Information System (hereinafter, IS) are monitored regularly, but at least once every 12 months;
- A DoORIS&BC employee may initiate unscheduled monitoring of access permissions to Exchange’s information systems in the event of an IS incident or other circumstances requiring revision of granted access rights;

- User IS access permissions are monitored as follows:
  - The DoORIS&BC employee requests from administrators of the IS concerned a list of all existing unlocked accounts and their access permissions;
  - From the list of accounts received for each of the IS to be checked, the DoORIS&BC employee randomly selects several accounts to further check their access permissions. The selection should include only accounts that have not already been checked in previous periods;
  - The DoORIS&BC employee asks the administrators of the access permission registration system for the applications residing in that system to grant access rights to users from the selection;
  - The DoORIS&BC employee checks the data provided to identify access permissions that have not been proven by the relevant applications;
  - if any breaches are identified, the DoORIS&BC employee initiates a process to study their causes and to choose appropriate corrective measures. Furthermore, all incidents of non-compliance are investigated in accordance with internal information security documents;
  - The DoORIS&BC employee performing such monitoring shall document the findings.

7.9. Defining and implementing measures to ensure that trading members and their clients, as well as other counterparties of the Exchange, provide the Exchange with information on their operational risk events related to their participation in organised trading.

Procedure for defining measures to ensure that trading members and their clients, as well as other counterparties of the Exchange, provide the Exchange with information on their operational risk events related to their participation in organised trading:

- The Exchange sets up a hotline for trading members and accepts calls to technical support in case of technical faults arising on the side of trading members;
- The Exchange supports the recovery of trading tools in case of problems on the side of trading members;
- The Exchange escalates the situation if the problems indicate a technical fault on the Exchange's side;

- The Exchange initiates a follow-up discussion, confirmation of measures to prevent recurrence of technical problems at the IT Committee.
  List of measures to ensure that trading members and their clients, as well as other counterparties of the Exchange, provide the Exchange with information on operational risk events related to their participation in organised trading:
- Including specific requirements for external trading software and hardware tools interfacing with Exchange's systems in the regulatory documents, stating the need for prompt risk reporting;
- Maintaining channels of communication and operational information with trading members, their clients and counterparties in order to arrange for information collection regarding identified operational risk events and measures taken to mitigate the negative impact of the risk;

7.10. Carrying out the monitoring of the use of trading tools by trading members.

Procedure for carrying out the monitoring of the use of trading tools by trading members includes the following:

- Monitoring of TCS as a whole and its particular elements, including customer connectivity parameters. The TCS monitoring system recovery process is identical to that of the system itself;
- In the event that the number of clients changes considerably, the responsible unit's employee, referred to as the Assistant Duty Employee, follows the specific instructions in the relevant system, which are tailored to each class of problem. These instructions shall be kept update on the results of operations, analysis of diverse situations, etc;
- Any customer-side software (external trading software and hardware) shall complete certification;
- Monitoring of the number of connections and behaviours of a trading member for a large number of incorrect transactions;
- If an abnormal situation is identified, which does not conform to trading members' normal behaviour, it is escalated by the Duty Employee for the respective system to the Duty Operations Director and Customer Support Department, who jointly address the problem that has arisen. CSD communicates the customer to clarify the

problem. DoT&SSM is entitled to initiate a procedure to disable trading for this customer in accordance with Moscow Exchange's Admission Rules in case of failure to contact the customer or if, after explaining the problem to the customer, the problem is not dealt with.

- If a loss of connection is registered beyond the scope of the trading mode, the number of lost connections is analysed and the need to suspend trading is assessed (if the number of lost connections is more than 50% of the total number of connections). The problem is escalated to the departments responsible for addressing the issue and an action plan is developed;
- Monitoring the quality of connectivity to external trading software and hardware tools, done on the provider's side.

7.11. Defining a list of requirements for the software and hardware used by trading members and their clients when connecting to trading tools.

Only external trading software and hardware tools certified on the test environment as compliant with the functional requirements of the systems and requirements for connection to the Exchange's software and hardware are allowed for the production environment.

7.12. Fixing deficiencies in the operation of the trading tools identified through tests on the trading tools.

- A test work report stating the findings and any deficiencies identified is produced at the end of the test work;
- If deficiencies are identified, they are recorded in the Jira system with a ticket assigned to them. The ticket is assigned to a particular release, or, if otherwise, a backlog is produced. The Development Manager of the system concerned is responsible for generating a backlog;
- Identified deficiencies in the operation of the trading tools are ranked according to the level of criticality: critical, high, major, minor, and deficiencies with no impact;
- The levels assigned are agreed on with the development team, which then decides on a plan of action for each identified deficiency and prioritises how to fix it. Critical and high-level deficiencies are treated first;

- If critical level deficiencies are identified during the testing phase, the release is not delivered until such deficiencies have been fixed. If so, a decision may be taken not to include in the release a task with critical deficiencies, or to postpone the release date until the relevant deficiencies have been fixed. Any critical deficiencies shall be reported to the Resource Committee (hereinafter, RC);
- The updates on testing status are reviewed at each RC meeting on a weekly basis;
- Also, when deficiencies in external trading software and hardware tools and/or monitoring tools are identified, these incidents are escalated to DoORIS&BC and reported as an operational risk event with the status to be tracked on a monthly basis.

7.13. The Exchange maintains the operational risk events database for the following types of operational risk events:

- events leading to suspension or termination of Exchange's processes which causes disruption of Exchange's procedures on organisation of trading, including suspension or termination of organised trading, both in respect of a particular financial instrument, foreign currency, commodity type and in respect of all mentioned instruments (hereinafter, the critical processes of the Exchange), including emergencies (hereinafter, material operational risk events);
- operational risk events other than those classed as material operational risk events, but according to Exchange's assessment posing negative effect on procedures and conditions of the Exchange's critical processes, including the ability to place orders, the ability to execute trades in relation to more than fifteen percent of trading members or their clients of the total number of trading members or their clients registered in the relevant trading (exchange) section, respectively (hereinafter, significant operational risk events);
- operational risks other than material and significant ones (hereinafter, low-impact events).

In addition, OREDB includes events other than material, significant or low impact events, that do not affect the Exchange's business but may potentially give a rise to operational risk events.

7.14. Training the employees of the Exchange to detect, assess and mitigate operational risks.

- All new hires to the Exchange receive mandatory training in identifying, assessing and mitigating operational risks before they get to work;
- The Director of DoORIS&BC delivers in-depth training to Exchanges employees on operational risk management, tailored to specific focus groups (based on the functions of the unit);
- It is compulsory for individual employees of the Exchange to take e-learning courses, that are made available on the corporate portal;
- DoORIS&BC monitors training statistics at least once a month.

7.15. If software and hardware tools of the Exchange are found inappropriate to the nature and scope of Exchange's operations, the Exchange takes efforts for their replacement or improvement (upgrade).

In order to identify the need to replace and/or improve (upgrade) the Exchange's software and hardware, load testing is undertaken on an annual basis. If any non-compliance is identified through load testing, a mix of measures is implemented, those including the assessment of the need for software upgrades and the implementation of upgrading measures.

Procedure to perform activities for replacement or improvement (upgrade) of Exchange's software and hardware tools if they are found non-compliant with the nature and scope of transactions performed by the Exchange includes:

- regular monitoring of Exchange's software and hardware facilities;
- annual load testing on Exchange's software and hardware facilities;
- analysis, monitoring and implementation of measures to upgrade Exchange's software and hardware facilities; If any inconsistency with the nature and scope of Exchange's transactions is found, software and hardware shall be upgraded or procured.

7.16. Within the operational risk management framework the Exchange has developed a system of measures designed to ensure uninterrupted operation of

Exchange's software and hardware, as well as to resume Exchange's activities in case of occurrence of operational risk events. These measures include:

- Determining the list of critical processes of the Exchange as well as processes of trading members and (or) contracting parties of the Exchange, the suspension or termination of which results in the interruption of the procedure for Exchange's operations for trading organisation, including the suspension or termination of organised trading, both with respect to an individual financial instrument, foreign currency or commodity and with respect to all of the above instruments.
- when developing Business Continuity Plans, each business unit specifies a list of critical processes that arise when interacting with counterparties, including the processes for interacting with Trading Members. Such interaction is assessed as part of the business continuity programme;
- Defining an action plan to respond to an abnormal situation arising on the critical processes of the Exchange, as well as on the processes of Trading Members and/or Exchange's counterparties;
- testing from time to time the adequacy and sufficiency of abnormal situation response efforts.

The list of critical processes of the Exchange is defined through the following:

- The list of critical processes of the Exchange is determined by DoORIS&BC jointly with business unit heads.
- The list of the Exchange's critical processes is described in BC&R Plans for business units directly by the business units jointly with the DoORIS&BC;
- DoORIS&BC regularly analyses external effect on business;
- DoORIS&BC jointly with the heads of business units list critical processes for business units;
- The list of critical processes is revised at least once a year.

7.17. Identification of emergencies and analysis of the circumstances in which emergencies occur.

Emergency control:

- Trading tools and normal functioning of all Exchange's processes are monitored continuously in order to detect anomalies and irregularities in the operation of Exchanges processes in a timely manner;
- Employees promptly notify all the persons concerned in Exchange's business units of all detected anomalies and irregularities in Exchanges processes;
- An abnormal situation may be recognised as an emergency by a decision of the authorised body responsible for coordinating actions to deal with the situation;
- The circumstances of an emergency/abnormal situation are analysed;
- Emergency/Contingency plans are activated;
- Development and further implementation of measures to minimise the negative consequences from abnormal situations to prevent their recurrence, improvement of abnormal/emergency siltation response plans;
- A list of potential abnormal situations is maintained to keep emergency/abnormal situation response plans up-to-date.

7.18. Ensuring uninterrupted operation of trading tools, including through control of the volume and frequency of orders received from trading members, which would result in the suspension or termination of organised trading services in full or in part.

The Exchange ensures uninterrupted operation of trading tools, including through control of the volume and frequency of orders received from trading members, which would result in the suspension or termination of organised trading services in full or in part. Control procedures include, inter alia:

- Monitoring of TCS as a whole and its particular elements, including customer connectivity parameters. The TCS monitoring system recovery process is identical to that of the system itself;
- In the event that the number of clients changes considerably, the responsible unit's employee, a Duty Employee, follows the specific instructions in the relevant system, which are tailored to each class of problem;

- Any customer-side software (external trading software and hardware) shall complete certification;
- Monitoring of the number of connections and behaviours of a trading member for a large number of incorrect transactions.

7.19. Determining the list of potential emergencies based on the Exchange's assessment of possible costs (losses), trading members and their clients, as well as its other counterparties due to any breach in the continuity of the Exchange's business, the probability and timing of such breach, and the nature and volume of trades carried out by the Exchange.

Threats that could lead to failure of trading tools are identified as part of the business continuity management at least once a year. Furthermore, the list of potential threats may be reviewed on an ad hoc basis due to changes in the international environment (sanctions), domestic political problems, economic, man-made and epidemiological situations and their impact on the financial standing of the Exchange. Potential threats already on the list may also be reprioritised due to changes in these circumstances.

7.20. Development and approval of a document outlining the measures to be taken by the Exchange in emergency situations and aimed at ensuring the continuity of activities relating to organisation of trading and exchange of Digital Financial Assets (hereinafter referred to as the Business Continuity Plan).

The Exchange has in place and approved Business Continuity Plan that outlines actions to be taken by the Exchange in case of emergency to ensure continuity of Exchange's operations relating to organisation of trading and exchange of DFAs.

The Business Continuity Plan is an internal document of the Exchange, which defines objectives, targets, procedure, methods and timing of the set of measures on prevention or joint elimination of the consequences of possible violation of day-to-day functioning of the Exchange (its business units) caused by unforeseen circumstances (occurrence of emergency situation or other event that is likely to happen, but hardly to predict and relates to a threat of significant financial losses or other consequences preventing the Exchange from fulfilling assumed obligations).

The Business Continuity Plan consolidates Exchange's business continuity documentation. Business Continuity and Recovery (BC&R) plans have been developed and introduced for each business unit of the Exchange. Business continuity measures developed for business units are consolidated, grouped, prioritised and form the framework for work instructions and consistent actions of the Exchange's staff in an emergency.

The Business Continuity Plan describes the operational processes and prioritises the activities of the Exchange from the announcement of an emergency till the moment when normal operations are resumed and the emergency is then cancelled, considering the worst-case scenario (main office is unavailable; primary data centre is unavailable; main office and primary data centre are unavailable).

The Business Continuity Plan is designed to ensure response actions to material incidents; it includes the assessment of possible consequences of an incident for operations of the Exchange, making decisions on activation of business units' response action plans, ensuring that the Exchange fulfils obligations before customers, prevention of possible interruption of day-to-day operations the Exchange, ensuring that the Exchange performs settlement and clearing transactions according to the undertaken obligations, maintaining the Exchange's management at the level that allows providing the conditions for making substantiated, optimal management decisions, their timely and complete implementation.

Objectives, targets, procedure, methods and timing of the set of measures on prevention or joint elimination of the consequences of possible violation of day-to-day functioning of the Exchange (its business units) caused by unforeseen circumstances (occurrence of emergency situation or other event that is likely to happen, but hardly to predict and relates to a threat of material financial losses or other consequences preventing the Exchange from fulfilling assumed obligations) are defined as part of managing business continuity risks.

7.21. The assessment of the business continuity plan to determine whether the measures it contains are sufficient to ensure the continuity of trading operations based on the nature of activities performed by the Exchange and the scope of transactions performed; if the insufficiency of these measures to ensure the continuity of business relating to organisation of trading is detected, the business continuity plan shall be reviewed.

The Exchange ensures that the following efforts are implemented:

- The Business Continuity Plan is reviewed at least every two years to verify that these measures included in the Plan are sufficient to ensure the continuity of business relating to organisation of trading.
- If these measures are found insufficient to ensure the continuity of business relating to organisation of trading, the Business Continuity Plan is revised.

Insufficiency of these measures and the basis for regular or extraordinary revision of the BC&R Plans for business units and the consolidated Business Continuity Plan are determined when and on the basis of the following:

- BC&R Plan testing findings and emergency training exercises
- changes in the structure of business units, their name, staff count, office location, area of activity or function, responsibility and authority of employees and personnel;
- changes in the location of equipment, scope of equipment and software under management or needed for the unit's activities;
- threat emerged or emergency event, based on an analysis of actions taken by particular business units and the Exchange as a whole, and the implementation of Business Continuity Plan measures in a given emergency situation.

7.22. Organising the operation of backup means of trading that functionally backs up primary trading facilities (hereinafter, the back-up office) that meets the following requirements:

- location of the back-up office in a detached building (outside of the principal complex of trading means);
- geographical remoteness from the primary trading facilities at the distance that ensures the ability of the Exchange's employees to continue working at the back-up office for an hour from the moment of occurrence of the emergency event;
- maintaining continuous operation of the back-up office and the possibility of switching the control to it if it becomes impossible to carry out the critical processes of the Exchange at the primary trading facilities.
- In the mandatory tests, workers are notified of the means of transport to the back-up office and of procedures to follow when they are in the back-up office.

7.23. Creating back-up copies of information contained in the registers which the Exchange is required to maintain in accordance with the Law On Organised Trading in the manner, amounts and time limits specified by the Exchange (but at least once a day), and keeping these copies for five years after their creation.

- Backing up:
  - Administrators decide on the method, scope and frequency of backups, select the type of medium on which backups will be made and decide on the use of cryptographic tools to protect the backed-up information based on the criticality of the information, special aspects of the use of information and business requirements, and as required by GOST R 57580.1-2017. These parameters shall be defined individually for each Information System (hereinafter, IS). The owner of IS information defines critical importance of such information.
  - Technical means that meet backing up parameters (method, scope, frequency, speed) are used for backing up.

- Storing the backup information:
  - The administrators, together with DoORIS&BC and IS owners determine the backup storage time for each IS. Minimum storage time is five years. Storage time is set based on the level of information criticality for Exchange's business processes and based on requirements of the Russian Federation legislation, those including regulatory and legal acts of governmental authorities responsible for financial market regulation, control and supervision;
  - Backups (external drives) are stored separately from the primary drive to minimise their simultaneous damage;
  - Access to the premises where backups are stored is restricted;
  - The storing conditions of the physical media comply with the manufacturer's specifications;
  - At the end of the storage period, information on external drives is deleted in accordance with the requirements of the Confidential Information Record, Storage and Destruction Procedure, and the drive is returned to use;

- At the end of useful life of external drives, the stored information is deleted and the drives are physically destroyed in accordance with the requirements for recording, storage and destruction of confidential information.

- Testing backups and restoration procedures:

  - Backups are regularly tested to ensure that there are no failures, so to ensure that information can be recovered should such a need arise;
  - The following checks are carried out as part of tests on backups:
    a) verification of integrity of backups carried with backup tools;
    b) randomly checking the recoverability of information from backups (for non-trading system data);
    c) restoring information from backups (for trading system data) on a regular basis;
  - The backup settings include a subsequent integrity verification;
  - For non-trading system data, a random check of recoverability is implemented so that at least 5% of the total number of backups with a storage period of one year or more are included during a year. A random check of recoverability also includes all data recovery cases in response to user requests. A backup is considered functional if it has been used at least once within a year to recover data;
  - The following actions are performed on data relating to ASTS trading system:
    a) for operational data, databases are backed up daily by means of database management system in use, with verification for readability (recovery) and correctness of the archive copies. restoring database from archive copies is carried out in accordance with the current regulations on technological operations of database reorganisation after a mass data update (deletion, modification), but at least once a month;
    b) for archived data, control of archive at the time of its creation is carried out by recovering the database from it. Thereafter, once the archived data has been saved on an external drive, these drives are checked for readability (restoration capability) at least once a year.
  - The following actions are performed on data relating to SPECTRA trading system:

a) replicating (mirroring) critical data and verifying its integrity by means of database management system in use;
b) daily data backing up with a subsequent restoration using a backup site
c) monthly archived data backing up and restoration.

- In all data restoration from backups cases, data integrity is verified by technical backup tools, including verification of the integrity of the information recorded on the medium when creating a directory;
- If a backup is found incorrect, the Administrator identifies and fixes the problem.

- Recovering information from backups:

  - Any recovery of information not caused by an emergency recovery related to loss of information system or its components function is made upon request submitted to the technical support service (helpdesk);
  - The information recovery process proceeds as follows:
    a) an employee who needs to recover lost information sends a request stating the reasons for the need for recovery to the helpdesk;
    b) An employee requesting to recover the information which he or she has not previously had access to must get approvals for that in accordance with the rules for managing access to information systems and procedures for changing access permissions;
    c) When an administrator receives a request to recover information, they follow the recovery procedure as specified in the request and notify the requester via the helpdesk of successful completion of recovery.

Procedures to control backup of data from registers kept by the Exchange according to legislative requirements (at least once a day) include the following:

- DoORIS&BC controls whether the backup process is successfully completed as follows:

  - A DoORIS&BC employee decides on information systems to be checked, restores a backup and checks the functioning of the hardware and software systems;

- then the Employee named above asks the Administrators for the results of the backup for the information systems selected for a given period of time, which is selected randomly by the DoORIS&BC employee;
- The DoORIS&BC employee who performed the audit shall draw up a report on the audit of backup procedures;
- At least once a year, is restored and the backup procedure is checked for proper functioning.

7.24. Checking that separate power generators for the primary trading facilities complex and the back-up office are available and maintained to supply power for critical processes of the Exchange for the entire duration of the Exchange's primary software and hardware facilities recovery.

- In the data centre buildings, diesel generator sets (hereinafter referred to as DGsets) are installed in separate rooms. Weekly, twice-monthly and annual maintenance procedures are carried out in accordance with the manufacturers' requirements;
- During the weekly maintenance, all DGsets are run without load. Technical parameters are checked according to the standard programme;
- During the twice-monthly maintenance, all DGsets are run without load. Technical parameters are checked according to the advanced programme using vendor's technical means;
- During the annual maintenance, all DGsets are run with a test load (external load device connected). Consumables (oil, filters, antifreeze, etc.) are replaced, technical parameters are checked according to an extra programme using the technical means of DGset vendor.

7.25. Creating and maintaining the technical tooling of the back-up office at the level necessary to ensure the resumption of Exchange's critical processes and possibility of commencing the works for migrating the critical processes of the Exchange carried out using the trading means from the primary complex of trading means to the back-up office in the manner and within the period established by the Exchange.

- As part of the annual testing procedure, employees test equipment in a back-up office;
- If any irregularities are detected, the problems identified are reported to the employee responsible for business continuity;
- Based on problem analysis, action plans are developed to address the problems identified.

7.26. Activities ensuring the possibility of provision of services necessary for operation of the primary complex of trading means and the back-up office by at least two independent suppliers of telecommunication services.

The Exchange makes arrangements ensuring that at least two independent telecommunication service suppliers provide services necessary for the operation of the primary complex of trading means and the back-up office. Arrangements to ensure that the services necessary for the operation of the primary trading facilities and the back-up office can be provided include:

- regular study of the market of the telecommunication services;
- quality assessment on existing telecommunication service providers;
- Introducing supplier accreditation procedures for access to trading facilities by telecommunication operators;
- maintaining several valid contracts with at least two telecommunication service providers, for the back-up office and the back-up data centre.

7.27. Keeping the back-up office at the level that ensures the possibility of functioning of all critical processes of the Exchange and maintaining such processes for at least one month from the emergency event occurrence

- Backup workstations are tested in accordance with approved schedule of BC program testing, but not less than once in the past 12 months;
- Following test results a report shall be generated and circulated among all interested parties;
- Back-up workstations shall be tested by business unit employees, for whom such workstations are assigned according to the seating plan of the back-up office.

Testing means evaluation of whether they meet unit requirements to equipment of back-up places, office infrastructure, and availability for restoration of vulnerable processes of the units within predefined time-frames, and so on.

In order to keep the back-up office at the level that ensures the possibility of functioning of all critical processes of the Exchange and maintaining such processes for at least one month from the emergency event occurrence the following requirements to back-up offices are met:

- the back-up office on the territory of the Russian Federation is located within a sufficient territorial distance from the main office to allow Exchange's employees to continue working in the back-up office within one hour after an emergency situation arises;
- separate electric power generators of sufficient capacity are available in the primary and back-up offices;
- at least two telecommunication service providers are available for the primary and back-up offices;
- it is ensured that the back-up office of the Exchange resumes its operations as soon as possible after an emergency, including the resumption of critical processes in the office within the planned (target) recovery time;
- as soon as an emergency occurs, it is ensured that critical processes involving the Exchange's software and hardware can be relocated from the main office to the back-up office without delay;
- the technical condition, technological and methodological support of the back-up office is kept at a level sufficient to enable all critical processes of the Exchange to function and to ensure that these processes can be sustained for one month from the time of the emergency;
- information and databases serving critical processes are backed up to backup media to resume such processes in the event of loss or damage of information or databases due to emergencies, and these backups are kept for five years from the date of their creation.

7.28. As part of managing its reputational risk, the Exchange collects and analyses feedback on Exchange's activities in the media, also through specialised automated information systems.

The Department of Marketing, PR and Customer Services collects and assesses factual information on reputational risks. Department of Marketing, PR and Customer Services and DoORIS&BC joint tasks:

- They build relations with mass media (print media, radio, Internet, etc.), including periodicals, radio, television, other forms of periodical mass media, including the Internet, and information received from business units of the Exchange, in order to collect and analyse press coverage on the Exchange, including information received through claims handling;

- Facts of reputational risks are checked for reliability and relevance. The expert assessment of information received is made by the Department of Communications as to what extent a damage caused to the Exchange's reputation hinders Exchange's objectives. Verification involves cross-checking information with information from another source;
- The unit responsible for collecting and analysing information on reputational risk facts is authorised to contact business units of the Exchange for confirming and clarifying information, inter alia, information on identified violations and orders from regulatory authorities, claims from clients, claims from regulatory and law enforcement authorities;
- Reputational risk assessment may involve analysing the effect of goodwill on the financial position, the effect of the Group companies' goodwill on the Exchange's goodwill, the effect from preventive and control measures (charity and public activities, advertising and information policy) on the Exchange's goodwill.

In assessing the level of reputational risk, the following factors may be taken into account:

- changes in Exchange's financial position (e.g. changes in the structure of assets, their impairment in total or in specific groups, changes in the structure of equity (capital);

- growing (decreasing) number of complaints and claims against the Trade Organiser, including those regarding the quality of services provided to customers and counterparties, and compliance with business practices;
- dynamics of the share of assets placed as a result of transactions with affiliates, subsidiaries in total assets;
- identification, as part of the internal control system, of non-compliance with regulatory requirements, including those on money laundering, as well as indications of possible involvement of the Exchange, Group companies, and Exchange's clients in money laundering;
- identified cases of Exchange's theft, forgery, fraud, Exchange employees' using confidential information obtained from clients and counterparties for personal purposes;
- refusal of regular or large clients and counterparties to cooperate with the Exchange.

The reputational risk is assessed and monitored on an ongoing basis, also through the following:

- regular review of the Exchange's performance indicators;
- monitoring the number of complaints and claims against the Exchange, including those regarding the quality of services provided to clients and counterparties, and compliance with business practices;
- monitoring positive and negative publicity and media coverage of shareholders and affiliates.

Measures to minimise the likelihood of reputational risk include:

- monitoring a business reputation of shareholders, affiliates and management of the Group;
- monitoring the accuracy of financial statements and other disclosures to shareholders, customers and counterparties, regulatory and supervisory authorities and other stakeholders, including for promotional purposes;
- existence of an information management system that prevents persons accessing such information from using the information for their own benefit and provides management and employees with information on negative and positive publicity and

reports about the Exchange from the media (periodicals, radio, television, other forms of periodic media distribution, including the Internet) and other sources; timely review, analysis of completeness, reliability and objectivity of the information provided; timely response to available information;

- taking disciplinary action towards employees caused increased reputational risk to the Exchange who committed a disciplinary offence.

In addition, to minimise the likelihood of reputational risk, appropriate measures to minimise operational risk are implemented as part of the risk management system in accordance with internal documents of the Exchange.

7.29. The Exchange, while managing its strategic risk, ensures implementation of the following potential risk sources identification measures:

7.29.1. Development of draft changes to organised trading procedures or activities related to organised trading, rendering additional services, admitting new financial instruments, foreign currency, commodities to organised trading and other organisational and/or technological changes (hereinafter, draft changes).

The procedure for developing change projects includes the following:

- For project initiatives, the initiator prepares an initiative document, gets approvals from with the head of the function (customer), and submits it to the Project Office;
- The Project Office centrally collects and registers all initiatives on changing and creating new processes in organised trading and other initiatives.

The single registration process seeks to harmonise collecting and evaluating initiatives to further optimise the allocation of the Exchange's limited resources between projects and tasks according to the Exchange's strategy.

The Committee for Technology Changes to Software and Hardware Facilities deals with the issues regarding control and management of changes to the IT infrastructure supporting Exchange's operations.

7.29.2. Feasibility study for draft changes.

- As part of draft changes and initiatives feasibility study, a register of initiatives is generated. The register is consolidated by DoRM&PO, the responsible business unit, and submitted to the Project and Product Committee, an advisory body to the Executive Board.
- DoORIS&BC jointly with FRMO and DoICC assesses risks attributed to project implementation and risks mitigated by the project for each initiative, and generates a statement on risks;
- The Finance Unit and project managers jointly calculate financials for each initiative (NPV, TCO, etc.);
- A risk report and a list of financial indicators are presented to the Project and Product Committee;
- PPC recommends to the Executive Board and the Executive Board decides on the implementation of projects, changes and prioritises initiatives.

Decisions are made by balancing between investment feasibility and economic benefits, and feasibility for mitigating the identified risks and improving the Exchange's performance.

7.30. Analysis of the effectiveness of implemented by the Exchange amendment initiatives following their implementation in the Exchanges activities.

Post-project (post-investment) monitoring is carried out to assess project success. Post-project monitoring is not a part of the project life cycle and can take place after all project activities have been implemented, including project completion.

7.31. Development planning efforts, including those towards developing the Exchange’s strategy for a period appropriate to the nature of Exchange’s activities and the volume of transactions to be carried out.

The Exchange carries out the following development planning activities:

- development of a five-year corporate strategy for the Exchange;
- development of a strategy roadmap;
- calculation of resources required to implement a strategy roadmap;
- approval of the corporate strategy by the Supervisory Board of the Exchange;

- The Supervisory Board of the Exchange may decide to amend the Exchange's corporate strategy.

7.32. The Exchange's corporate strategy is assessed to find out whether it is feasible and expedient to implement, and if the Exchange so decides, the corporate strategy is amended.

The Exchange assesses its strategy to determine whether it is feasible and expedient to implement using the following procedure:

- identifying risks to achieving strategic objectives;
- identifying risks to the Exchange's strategy;
- assessing risks to achieving the objectives;
- assessing risks to the Exchange's strategy;
- bringing these risks to the Supervisory Board for consideration so that they determine whether it is expedient to revise the Strategy;
- monitoring of the identified risks throughout the implementation of the Strategy.

The Exchange's assessment of its strategy involves:

- assessing strategic options developed to verify their appropriateness;
- comparing strategy assessment results;
- making changes to the Exchange's development strategy, if necessary.

Key assessment criteria:

- consistency in strategy implementation;
- consistency with environment requirements;
- feasibility;
- acceptability to pressure groups;
- competitive advantages.

The strategy evaluation is the final stage of strategic planning. It continues through all stages of strategy implementation, including the assessments of the specific strategic options generated to determine their suitability, feasibility, acceptability and consistency for the Exchange.

7.33. Develop and approve a document defining the measures to be taken by the Trade Operator for maintaining and recovering financial sustainability of the Trade Operator to ensure continuity of critical services (Financial Sustainability Recovery Plan, FSRP).

The Trade Organiser has developed and approved a Financial Stability Recovery Plan, aimed at developing early actions and measures to maintain and recover financial stability of the Trade Organiser to ensure continuity of the Trade Organiser's critical services in case of material impairment of its financial position, as well as measures to avoid and prevent worsening of its financial position using available instruments and methods.

The FSRP assesses the ability of the Trade Organiser to counter stress events that could have a negative impact on its financial stability and ability to provide critical services through options other than public funds and Bank of Russia funds.

The FSRP considers options (scenarios) for the loss of financial stability of the Trade Organiser and describes conditions that will trigger measures to prevent impairment of the Trade Organiser's financial position and to recover financial stability, as well as the decision-making process to initiate these measures.

The FSRP covers measures taken to supplement capital and maintain liquidity in the event of one or more unfavourable scenarios for the Exchange implemented, including those associated with a worsening in the financial position of its strategically important subsidiaries. Implementation methods are defined for each scenario, including scenario-specific indicators, early response measures and recovery measures.

8 Procedures to ensure control of processes and measures to identify, analyse and monitor risk, share information across business units and corporate bodies of the Exchange, as well as procedures to implement processes and measures carried out by the Exchange in managing certain types of risks of the Exchange

The Exchange controls risk analysis and identification processes through the following:

- regular tests on the trading tools to help identify potential risks associated with abnormal operation of TCS;
- inventory of software and hardware, which takes place every three years to monitor the replacement or improvement (upgrade) of Exchange's software and hardware tools if they are found to be inadequate to the nature and scope of Exchange's operations;
- independent control of the main processes used to create and operate automated systems that are part of the trading tools, including information security control on compliance with the requirements of the documents developed within the framework of the legislation of the Russian Federation on technical regulation taking into account the provisions of international standards (operational audit), at least once every two years with the involvement of independent consultants;
- independent certification audit on ISO 22301 compliance of the test work process (testing) of the trading tools as well as the procedures for correcting deficiencies identified as a result thereof an annual basis;
- periodic audits by IAS;
- periodic revisions on particular processes by DoORIS&BC, ICS and DoICC
- control procedures by other business units;
- analysis, assessment and development of follow-up responses to the results of control procedures, documenting the results, and reporting by DoORIS&BC staff or other business units managing specific types of risks;
- decision-making by the Exchange's authorised corporate bodies based on the results of risk reporting review. At different risk management stages, these functions are carried out by the Director of DoORIS&BC, the Head of FRMO, and by the Executive Board;
- The Exchange arranges for risk management system adequacy verification by IAS, independent audit companies and by supervisory authorities.

The control phase of the risk management process ensures that the Exchange's governing bodies are fully informed and paves the way to management decisions.

The control process as part of the risk management process comprised of the following activities:

- development and implementation of automated control procedures;
- formulation of plans for non-automated control procedures: definition of control objects (processes, measures, activities of business units), control procedures (as part of self-assessment, review/audit, request, etc.) and their deadlines;
- execution of control procedures in the reporting period;
- collection of information and data at the end of the reporting period, their aggregation by type of risk, analysis, assessment and reporting;
- Submitting reports to corporate bodies of the Exchange for decision-making;
- additional control procedures on the performed activities to analyse their sufficiency;
- periodic review and improvement of control procedures as part of performance and effectiveness evaluation of the risk management system.

9 Procedure for including Exchanges risks and results of risk assessment in the risk register, assessing the risk register for its relevance, and, should irrelevant information be identified in the risk register, procedure for risk register revision

Each employee of the Exchange shall report risks to DoORIS&BC as soon as such risks are identified.

After receiving a risk report, a DoORIS&BC employee analyses and assesses the risk based on its likelihood of realisation and the amount of possible loss, impact on processes, systems and other types of risk, assessment of the adequacy of applicable control procedures, possible risk response strategy, assesses for possible breach of risk level limits and escalates information to the management bodies of the Exchange, if necessary. If necessary, a DoORIS&BC employee may involve employees of business units responsible for managing certain types of risk.

After the analysis is completed, information on non-financial risks is entered into RD by a DoORIS&BC employee.

As soon as risk information appears and is recorded in RD, a DoORIS&BC employee monitors that the person responsible for the implementation of risk mitigation control measures executes the measures in due time, if any decision to mitigate the risk has been taken.

After the implementation of risk minimisation measures, it is analysed whether the measures taken close the risk or mitigate it. In the latter case, the risk is made subject to an annual inventory. In some cases, KRIs are implemented to monitor the mitigated/accepted level of risk.

If an annual RD inventory confirms to an DoORIS&BC employee that the risk is closed/out of relevance, he/she marks the relevant status on RD, thus removing the closed/out of relevance risk from the subsequent cycle of the annual inventory.

An employee of DoORIS&BC regularly checks RDB for its relevance and, if irrelevant information is found, revises the risk register of the Exchange at least once a year.

The following processes and procedures are used to discover and identify risk:

- collecting information on risks (both internal and external) that may cause damage to the Exchange and the factors contributing to those risks (including through self-assessment), collecting information on risk events and the factors contributing to those risk events;
- examining any possibility/likelihood of risks in the Exchange's activities, and of damage (in expected, worst, and most frequent amounts);
- diagnostics of business processes to identify points (nodes) of risk occurrence, analysis of overlapping powers and responsibilities of departments and employees of the Exchange;
- analysing the outcomes of internal and external audits performed on controls/procedures/systems;
- analysing new products, processes and systems (perform analysis of all innovations implemented by the Exchange: changes in structures and procedures, launch of new services and technologies, development of new lines of business, etc.);
- applying scenario analysis to identify threats that, in the Exchange's opinion, may lead to failure of trading tools and/or other reason for termination of activities for organising trades;
- using results from stress testing on software and hardware tools used for organising trades at intervals determined by Exchange's internal documents, but at least once every six months.

For each type of risk within the Exchange's risk management system, there may be a variety of risk identification methods that are specific to that type of risk.

10 Procedures for maintaining a database of operational risk events

The Operational Risk Event Database (OREDB), which covers, among others, such cybersecurity risks as computer attacks and facts (indicators) of compromised objects of informatization is managed on a regular basis as and when operational risk events are identified, in the following order:

- Responsible DoORIS&BC employees collect data on the event occurred. Each employee of the Exchange is obliged to report the event in the manner described in this section;
- If an event occurs:
  a) An employee of the Exchange who has knowledge of the event notifies his/her line manager and a responsible employee of DoORIS&BC not later than on the day on which the event is discovered;
  b) If complete information about the event is not available (the event is not complete and the information provided needs to be tracked), an employee submits all currently available information to DoORIS&BC.
  c) A responsible DoORIS&BC employee initially analyses the event information within the limits of his/her authorisation and, if the event is regarded as an operational risk event, performs the following actions:
     - analyses the operational risk event notice to see if there is any overlap of information (in OREDB);
     - classifies an operational risk event in accordance with OREDB classification guide;
     - records an operational risk event and assigns it a unique number.
  d) During the working day of registering an operational risk event, a Risk Manager clarifies with a Risk Owner the impact assessment, analyses and evaluates the operational risk event in order to assess the materiality of the event's impact on Exchange's activities and subsequently decides on measures to minimise the likelihood of a recurrence of the operational risk event;

e) On a regular basis, a Risk Manager independently or jointly with a responsible employee (owner of the risk where an operational risk event occurred) analyses the possible outcomes of events in OREDB and RDB, i.e. those negative consequences to which the events could potentially lead, but did not.

The results of such analysis are used to define stress-testing scenarios, in scenario and what if analysis, in developing a risk matrix of possible causes and likely outcomes, in constructing a risk map and risk matrix, and in forecasting.

A Risk Manager monitors and has the responsibility for ensuring that information about an operational risk event in OREDB is complete and up-to-date.

DoORIS&BC controls completeness and relevance of data on costs (losses) incurred by the Exchange from operational risk events on a daily basis.

11 Procedures and frequency (at least once a year) to detect threats which may, according to the Exchange's assessment, result in the failure of trading facilities

The Exchange identifies threats that according to the Exchange may lead to failure of means of trading, and continuously monitors the current status of means of trading, in particular, with respect to the need to update them;

Procedures to detect threats which may, according to the Exchange, result in the failure of trading facilities include the following procedures:

- identification of sources, factors that may lead to interruption of trading tools operation and their analysis;
- classification of threats followed by an assessment of their likelihood;
- load and penetration test on software and hardware suite;
- continuous monitoring of the current status of means of trading, in particular, with respect to the need to update them;
- yearly detection of threats which may result in the failure of trading tools;
- Determining the list of software and hardware tools of the Exchange that require protection against illegal actions, whose failures and/or errors may result in the

partial or complete suspension or termination of organised trading services and/or have another negative impact on operations of the Exchange.

- creation of a list of information security measures and their implementation in compliance with legislation requirements includes the following activities:

These actions are performed within the scope of business continuous management implemented and maintained by the Exchange, which operates in accordance with national legislation requirements, the requirements of the regulator, and in accordance with recommendations of international IS standards.

To identify threats to business continuity, business continuity risk management measures are implemented in the following order and with a specified frequency:

- Identification of business continuity threats requires that the Exchange's activities be viewed as a single interrelated mix of diverse activities performed by separate business units. Specialisations of individual business units feature continuity-critical procedures and functions, where failure to perform routine work inevitably leads to interruption and failure in operations of other business units, up to suspension of their activities, as a business impact analysis is carried out;
- A business continuity risk assessment is the next step after completion of a business impact analysis. Whereas a business impact analysis analyses the impact of failures in business unit processes on the business of the Exchange, a risk assessment shows what threats the Exchange in general is exposed to in a given period and how these threats may lead to failures in critical processes. The business continuity risk process includes the following:
  - identification of areas, work processes and functions that may expose the Exchange to business continuity risks;
  - identification of continuity threats which may lead to failure of normal operations in critical sub-processes and procedures identified throughout the business impact analysis;
  - analysis of the extent to which threats, if they occur, affect the Exchange, in particular, its employees, infrastructure and information assets;
  - assessment of the likelihood of a business continuity threat;
  - analysis of existing control procedures

- The continuity risk assessment process assesses the likelihood of threats, possible impact on the Exchange and existing organisational and technical measures, and control procedures to mitigate risks;
- Business continuity risks are assessed on a regular basis, both as part of annual review of management's business continuity management activities and in the event that there are substantial changes in the internal and external factors affecting continuity.

Procedures for monitoring the current status of means of trading, in particular, with respect to the need to update them includes the following:

- Monitoring a trading and clearing system (TCS) as a whole and its particular elements, including customer connectivity parameters. The TCS monitoring system recovery process is identical to that of the system itself;
- Any customer-side software (external trading software and hardware) shall complete certification in accordance with ETSH Certification Regulations and the Exchange's Requirements for interfacing ETSH with software and hardware of the Technical Centre;
- If threats are identified that may lead to failure of trading tools, the Duty Officer for the relevant system analyses and escalates the problem to the appropriate business unit. For more specific classes of problems, instructions have been developed that outline the actions employees should take to respond to such problems. These instructions shall be kept update on the results of operations, analysis of diverse situations, etc;
- If an incident is identified, information is also submitted to DoORIS&BC and analysed.

Threats which may, according to the Exchange, result in the failure of trading facilities, include the following:

- failure of technical means, failure of information systems (also as a result of technical failure) used to serve critical processes;
- disruption of utility infrastructure (water flooding of the Exchange's premises, in particular, due to pipe break etc);
- power supply outages (including those caused by failure of power suppliers to fulfil their obligations) that cannot be fixed by technical means available to the Exchange;

- disruption of communication channels (also caused by technical failure, refusal of the communication channel provider to fulfil contractual obligations.

other circumstances that, in the MOEX's opinion, may cause critical processes to be suspended or discontinued:

- notification from the Clearing Centre to the Exchange of an emergency that may lead to a disruption of services to trading members;
- attempts by third parties and/or in-house perpetrators to gain unauthorised access to protected information, or intentional creation of circumstances that affect the normal functioning of the Exchange's software and hardware (network attacks);
- adoption of or any changes in legislative or other regulatory acts of Russian governmental authorities or Bank of Russia's regulatory acts, as well as delivery of instructions and orders, statements, letters, telegrams, other acts of the said authorities that temporarily or indefinitely have made, make or may make it impossible or significantly hinder activities, as well as delivery of other significant services that used to be performed before adoption of the said acts.

12 Procedure for maintaining a database of expenses (losses) incurred by the Exchange as a result of operational risk events

The Exchange keeps a database of expenses (losses) incurred by the Exchange as a result of operational risk events (which covers, among others, such infosecurity risks as computer attacks and facts (indicators) of compromised informatisation objects) as part of maintaining a single OREDB on a regular basis as and when information is identified. Along with general details of each operational risk event, OREDB contains the following information:

- amount of expenses (losses) incurred as a result of an operational risk event;
- type of loss (direct, indirect, near miss);
- status of loss (reserve, write-off);
- risk source;
- type (area) of activities;
- recovery of loss;
- date of an operational risk event, which caused expenses (losses) to the Exchange;

- analysis of circumstances leading to occurrence (identification) of an operational risk event for the Exchange that resulted in expenses (losses) and of whether it is possible to cover expenses (losses).

Therefore, a single OREDB both satisfies the requirement to manage a database of expenses (losses) incurred by the Exchange as a result of operational risk events and contains all material information on operational risk events that allows for addressing the consequences of operational risk events and planning actions and long-term measures to manage this risk in the most effective way.

The minimum period of keeping the information on the expenses (losses) incurred by the Exchange due to the Exchange's operational risk events implication is 10 years.

13 Rights and obligations of Exchange's management bodies, heads and employees of Exchange's business units, including a company official (head of a business unit) responsible for organising the risk management system, as well as a company official responsible for operational risk management (if any), within the risk management framework.

Risk management is exercised at all levels of the Exchange and involves all management bodies and employees, with roles and functions delineated and at the same time complementary to each other. The duties and responsibilities for making and implementing (executing) risk management decisions are assigned to the participants of the risk management system in such a way as to avoid overlapping of functions, but to ensure risk management consistency and effectiveness.

The risk management system of the Exchange specifies the powers and functions of the risk management business unit and corporate bodies of the Exchange in organising and managing the risk management system.

- DoORIS&BC is responsible for the risk management system of the Exchange, particularly for the management of operational risk, including information security and business continuity risk, strategic, reputational and model risks.

  As part of managing certain types of risk, DoORIS&BC engages:
- FRMO team in terms of financial risks, in particular in relation to transactions with own assets;

- ICS team in terms of regulatory risk management in accordance with approved documents;
- DoICC team in terms of compliance risk management;
- Legal Department team in terms of legal risk management;
- Department of Communications in terms of reputational risk management;
- Strategy Department in terms of strategic risk management;
- The PO in terms of project risk management;
- The Tax Group team in terms of tax risks management.

The Director of DoORIS&BC, Business Units Heads referred to herein may serve on committees and commissions which are not structural units of the Exchange.

For the Director of DoORIS&BC, Moscow Exchange is a primary place of employment.

The Director of DoORIS&BC, employees of business units referred to herein are entitled to demand information (documents), including written explanations, from employees and Exchange's company officials on the matters arising in the course of performance of their duties.

Responsibilities of DoORIS&BC Director include, but are not limited to:

- development of training (consultancy) programmes for Exchange's employees on risk detection, identification, assessment and control;
- development of risk management methodology and tools;
- assessment of Exchange's risks considering the likelihood of risk occurrence and its impact on trade organisation activities;
- development of recommendations to corporate bodies, company officials, including heads of business units of the Exchange, on the measures to be taken to address a particular risk for the Exchange;
- control over measures implemented to mitigate Exchange's risks;
- providing risk information to the Exchange's collegiate executive body and the Exchange's Sole Executive Body;
- taking other measures intended to organise the risk management system in accordance with internal documents of the Exchange.

The Supervisory Board is responsible, among other things, for matters relating to the organisation of the risk management system, in particular:

- definition of principles and approaches to establishing a risk management system;
- approval of documents that define the Exchanges risk management policy;
- approval of documents that define the rules for organising the risk management system of the Exchange;
- approval of the Exchange's Risk Limit (Acceptable Risk Level) and Total Risk Limit Methodology;
- approval of a document outlining the measures to be taken in emergency situations and aimed at ensuring the continuity of activities relating to organisation of trading.
- approval of risk appetite metrics (benchmarks);
- approval of RMS performance indicators assessment;
- consideration and analysis of RMS performance indicators assessment;
- making the decisions driven by the results of the analysis and evaluation carried out.

In order to ensure that the decisions of the Supervisory Board are implemented in accordance with approved internal risk management documents, the Chairman of the Executive Board and the Executive Board implement the following measures:

- allocating risk management authorities and responsibilities among the Heads of Exchange's business units to comply with the main risk management principles;
- creating and maintaining an effective risk management system
- ensuring the organisation of the risk management process, including the formation of working bodies, including committees, commissions, the definition of their competence, approval of regulations on them;
- creating and maintaining an effective risk management system
- approval of credit and market risk limits (limit statement);
- approval of risk reporting.

The Risk Management Committee reviews the following documents before they are approved by the Supervisory Board:

- documents that set risk management principles;
- criteria to assess the performance of the Exchange's risk management system;

- documents that set key risk indicators, including risk appetite and the level of risk tolerance;
- reporting documents on the performance of risk management system.

All employees of the Exchange are obliged to report all risks and risk events that they have become aware of, and to provide information as requested by DoORIS&BC.

Heads of business units performing risk management functions shall analyse events and risks, ensure operation of the system and response in cases when thresholds and control values of risk appetite are exceeded.

The heads of risk management departments are entitled to receive a complete information on risks from business unit employees.

The risk management authorities belonging to business units are defined in the internal documents of the Exchange, including the regulations on business units.

Due to material functional interdependence the companies of the Moscow Exchange Group have, business unit heads who are responsible for the risk management of the Moscow Exchange Group on the permanent basis exchange information on the events and identified risks and also on the methods applied to their mitigation.

The Executive Board may establish collegiate consultative and advisory bodies (hereinafter, the Committees) that may include risk management coordinators of the Moscow Exchange Group's companies.

The Committees are created to resolve, inter alia, the following matters:

- implementation of the approved approach to the enterprise risk management across the Group companies;
- ensuring planning for interdepartmental interactions across the Moscow Exchange Group when implementing risk identification, assessment and analysis procedures;
- analysis of the events and facts that may threaten the customer's interests or have an impact on the financial stability, reputation of companies of the Moscow Exchange Group, determining their reasons and developing recommendations for their elimination.

14 The procedure for determining a separate responsible employee for the implementation of measures carried out by the Exchange as part of risk management, and the procedure for his/her interaction with the employee (separate business unit) responsible for organising the risk management system, in case the Exchange decides that such a person should be appointed

A separate business unit responsible for the implementation of the risk management system is established through an Order of the Chairman of the Executive Board and approval of Regulation on DoORIS&BC by an Order of the Chairman of the Executive Board.

DoORIS&BC Director's compliance with qualification requirements is checked. The DoORIS&BC Director's position shall be agreed with the Bank of Russia.

Employees responsible for managing individual risks are appointed by an order of the Chairman of the Executive Board.

Employees responsible for providing information on operational risks and operational risk events are appointed by an order of the Chairman of the Executive Board. They are all employees of the Exchange.

Employees responsible for implementing individual risk mitigation measures implement these measures by virtue of their job responsibilities.

15 Procedure and frequency for exchanging risk information between Exchange's business units, between Exchange's business units and corporate bodies, including procedure for communicating the action plan and information on its implementation, as well as information on risk limitations and breaches of set limitations, to Exchange's corporate bodies

The procedure and frequency for sharing information on Exchange's risks between business units of the Exchange shall include the following:

- Business units share risk information on a daily routine basis;
- DoORIS&BC notifies business units affected and business units involved in risk mitigation efforts of the risk identified at the time the risk is detected;

- If a threat, high risk or high-level impact event is identified, the information is escalated to the management authorities on the day of detection. Otherwise, information is communicated as part of regular reporting;
- Working groups meet at least once a month with regard to risk event analysis, risk level assessment and the status of risk mitigation measures. DoORIS&BC necessarily participates in such meetings. The meeting procedure is as follows:
  - Operational risk events that occurred during a reporting month are analysed and discussed;
  - Analysis of action status regarding events identified in previous periods.
- Risk information is subject to an annual inventory round as part of risk self-assessment;
- DoORIS&BC submits a report on the results of load testing to responsible IT business units no later than 10 days from the date of the report;
- In the course of risk identification, assessment, monitoring and control, DoORIS&BC informs Exchange's employees of the identified risks attributed to operations of the relevant business units to the extent necessary for the effective participation of employees in the risks assessment and generation of action plans for their mitigation and/or control.

Procedure for sharing information on risks between business units and corporate bodies of the Exchange is performed through regular and unplanned (ad-hoc) risk reporting.

The procedure and frequency for exchanging information on risk mitigation actions shall be as follows:

- As part of regular reporting, information on risk mitigation activities is made available to corporate bodies of the Exchange.
- The Group companies exchange information to ensure transparency of individual companies' processes and procedures, as well as effective interaction across Group companies in both ongoing activities and project activities.

16 The procedure and frequency (at least once every three months) for preparing and submitting reports and information to corporate bodies of the Exchange on the outcomes from processes and measures taken by the Exchange to manage individual types of risk as part of its risk management system

The governing bodies of the Exchange receive full and timely information, including reports on non-financial and financial risks respectively, from the Director of DoORIS&BC and the Head of FRMO in accordance with the deadlines and procedures set out in this section of the Rules.

Reporting comprises of regular and extraordinary (ad-hoc) reports.

Regular reporting includes the following reports:

- Reports on financial and non-financial risks make a part of Group risk reporting delivered by DoORIS&BC to the Executive Board and the Risk Management Committee at the Supervisory Board on a quarterly basis.
- Risk-appetite reports delivered by the Director of DoORIS&BC to the Executive Board at least once a month;
- .

The procedure for risk reporting is described also in the Financial Risk Management Policy.

Extraordinary (immediate) reporting is generated in the event of identified high-loss risk events, material changes in the risk level, in the event of breaches in risk limitations, and if additional special risk assessment programmes are implemented.

The Director of DoORIS&BC delivers information on an identified high-loss risk event, a material change in risk level, or additional special risk assessment programmes is submitted to the Exchange's Executive Board and the Chairman of the Executive Board no later than ten days after the relevant breach is identified.

All other users are provided reports by decisions of Exchange's governing bodies, except in cases where such reports are provided as required by federal laws and regulatory acts of the federal executive body for financial markets adopted in accordance with such laws.

The risk reporting system is designed to ensure the completeness, reliability and timeliness of risk information for all lines of business and the products and services offered. Risk reporting must be clear and contain necessary and sufficient information for effective management decisions.

17 Content of reports and information on the results of the implementation of risk management processes within the risk management framework submitted for consideration to corporate bodies of the Exchange

Regular reports on risks comprise the reporting forms approved by internal documents of the Exchange as well as the analytical portion, where the produced results are interpreted and recommendations are given with respect to the risk management activities.

Regular non-financial risk reporting includes:

- assessment of risks in the main areas of Exchange's activities, assessment substantiation, including information on Exchange's violations of the Law on Organised Trading, regulatory legal acts of the Bank of Russia adopted in accordance with the Law, the Charter of the Exchange and internal documents related to organising trades;
- measures taken to address the identified violations and mitigate risks;
- data on fulfilment of recommendations;
- information on material non-financial risk events;
- information on risk appetite monitoring indicators, detected limitation breaches (if applicable);
- other data stipulated by internal documents of the Exchange.

The content of regular financial risk reporting is disclosed in the Financial Risk Management Policy.

Extraordinary (immediate) reporting is generated as a Report of DoORIS&BC Director in the event of identified high-loss risk events, significant changes in the risk level, additional special risk assessment programmes implemented.

Reports generated from the load testing results include:

- information as to what release the in-house load testing was performed on;
- information on average and maximum values achieved with different thresholds for transactions per second;
- opinion on whether the functionality of the system is correct.

The load testing protocol is generated about 3-4 days before the release date, before each release of the Trading and Clearing System (hereinafter referred to as TCS). Reporting is provided to testing staff, Release Planning staff and is added to the scope of release documents.

Reporting on the results of DR testing gives a chronology of the analysis done and the observations that were exposed during the testing.

Reporting is generated when test results are obtained. Tests are conducted at least once a year and are necessarily disclosed to internal test takers.

Reports generated from the results of penetration testing include:

- report on the information system security analysis performed;
- list of weaknesses, vulnerabilities, risk analysis;
- recommendations to address and mitigate risks.

Reports are generated as testing progresses (pre-versions), after the penetration test has been completed and when the final versions are produced.

The consumers of these reports are: the owners of the information system under examination, the business owners, the technical owners and DoORIS&BC.

18 Procedures for managing risks associated with external services delivered by providers throughout the period of services, where the Exchange contracts external services with service providers

Operational risk management features the process of managing the risks associated with the provision of external services by service providers throughout the period of service provision. Contracting external services by the Exchange with service providers entails the following risks:

- failure to provide services properly;
- failure to provide documents confirming the fact of performance of the contract;
- violation of other conditions of the contract by the supplier, including violation of the confidentiality agreement, provision of false information.

Procedures for managing risks associated with delivery of external services by service providers:

- In order to manage risks associated with services delivered by service providers, providers are assessed, including verification of the accuracy of information provided by the counterparty, analysis and evaluation of its financial soundness, reliability and business reputation;
- Potential use of substitute suppliers is studied;
- Based on the results of the verification, a conclusion shall be made as to whether to enter into contract with the given counterparty;
- If the Exchange concludes an agreement on services related to organised trading activities (hereinafter, external services), with a third party (hereinafter, the service provider), the risk management system ensures that the Exchanger is provided with information and documents generated by the service provider in connection with provision of external services, as well as the management of risks related to the provision of external services by the provider during the entire period of services.

19 Self-assessment procedure and frequency (at least once a year), procedure for documenting findings of self-assessment

Risk self-assessment is a risk management tool that is used to detect (identify) risks, analyse and assess them, and to assess controls and define responses to risks. The decision on responding to operational risk, information security risk and business continuity risk is made and approved by Director of Operational Risks, Information Security and Business Continuity Department, and in some cases may be made by authorised collegial bodies.

The purpose of the Self-Assessment is to identify and assess non-financial risks inherent in Exchange's operations. The self-assessment is a team effort made by the Risk Manager and heads/employees of Exchange’s business units.

The self-assessment delivers expert information on the types and extent of inherent risk, control procedures in place to prevent it, and their effectiveness. The Self-Assessment identifies and assesses risks and controls on the basis of the expert opinion given by the heads/employees of business units within the scope of their functions and tasks.

The information obtained in the Self-Assessment is used in assessing operational risk as part of a proactive approach to risk management, including scenario analysis, stress testing, predicting potential negative outcomes from risk occurrences, what if analysis, building a risk map, determining risk appetite monitoring metrics, assessing effectiveness and improving control procedures, etc., and may be included in regular risk management reporting.

Self-assessment allows for a few important tasks in establishing effective risk management:

- identifying risks before they are implemented;
- raising awareness of risk management issues among non-core staff;
- Identification of missing or excessive control procedures, areas of control that are not in proportion to the business processes of business units.

Self-assessment is performed on a regular basis at least once a year and also when new products are launched, new business processes change, or when the Risk Map needs to be updated. Self-assessment also involves updates on risk in RD.

The self-assessment may use information from the external and internal data bases as well as the results from the previous self-assessment.

Key functional roles of participants in the operational risk self-assessment:

- Expert;
- Risk Manager;
- Risk Business Owner;
- Risk Owner;
- Plan Coordinator.

Key roles for participants in the operational risk self-assessment process.

An Expert participates:

- in questionnaire surveys (interviews) as part of the self-assessment process;
- expert assessment of the severity of losses from potential risk scenarios implemented (self-assessment).

Any employee, including the Business Risk Owner and the Risk Owner is eligible to serve as an expert. There are also risk experts, Heads of business units responsible forfor managing specific types of risk (financial, legal, tax, etc.). The role of risk experts is important in assessing the effect of risk types on each other and on processes in general.

A risk Manager defines the following:

- the level of self-assessment (top management, line management, individual lines of business, units or individual business processes);
- dates of Self-Assessment;
    f) a list of sources of information to form the final statement on the Self-Assessment. The most important source of information for identifying and assessing risks is the professional judgement of employees. Operational risk events detected, control test results, data of key risk indicator analysis, internal and external audit results, operational risk stress testing, information on risks associated with new project launches (product risks), information that is identified in claim management, etc. may also be used.

A Risk Owner is involved:

- in making a risk response decision and informing a Risk Manager of the decision;
- in monitoring the level of risk, if necessary, informing a Risk Manager of the results of monitoring;
- in assessing whether the existing risk avoidance controls are effective, and in developing improvement proposals where necessary;
- in ensuring timely implementation of risk minimisation and control measures, or identifying a person responsible for the implementation of measures.

The decision on whether to escalate risk responding to a higher management level is made by a Business Risk Owner based on expertise or on relevant internal documents, if available.

If it is decided to accept risk, a Risk Business Owner develops a plan to monitor this risk (a response decision may be re-decided based on monitoring results).

If it is decided to transfer risk, a Risk Business Owner initiates procedures to develop risk transfer mechanisms.

If it is decided to avoid/retain risk, a Risk Business Owner develops a plan to monitor this risk, assess whether control measures are effective or to reduce business activity in that area.

If it is decided to minimise risk, a Risk Business Owner initiates an assignment to the Risk Owner to develop plans to implement control procedures (risk mitigation measures).

A Risk Owner is involved:

- in developing and implementing a risk mitigation plan;
- in informing a Risk Business Owner or a Risk Manager directly of the status of measures to prevent risk and/or to improve existing controls.

The risk mitigation plan is agreed on with a Risk Manager and a Risk Business Owner. It is approved in accordance with the internal documents and submitted to a Risk Manager, who regularly monitors implementation of control procedures plans (situation reports are submitted to the Risk Business Owner, Risk Owner).

The Risk Manager coordinates a self-assessment procedure, gives methodological support and advises the participants of self-assessment.

Self-assessment shall be in the form of interviews and (or) survey among responsible business units to identify risks and prepare a self-assessment report outlining the risks identified.

A Risk Manager informs the Heads of business units on the dates of Self-Assessment by e-mail.

A Risk Manager coordinates a schedule of meetings with business unit employees or arranges for the Self-Assessment procedure in absentee format (questionnaires).

In the Self-Assessment process, employees and a Risk Manager, identify the following aspects:

- risks and processes that exist for a business unit in a business unit in particular, or for the Exchange in general, or operational risk events that are likely to occur;
- factors and sources of risk and the reasons for risk occurrence;
- significance of each risk (severity of consequences);
- probability/likelihood of risk;
- impact on other types of risk (compliance, regulatory strategic and reputational risks, legal and project risk);
- assessment of potential risk consequences in terms of assessing the financial effect on the financial strength of the Exchange by assessing the risk event(s) which, if occurred, including the probability of occurrence and degree of effect, will result in costs (losses) for the Exchange;
- assessment of the potential risk consequences in terms of effect on business continuity, i.e. occurrence of consequences involving suspension or termination of organised trading services in full or in part.

When analysing, a Risk Manager determines the inherent level of risk for each risk (before controls are implemented), the residual level of risk (with controls in place) and the target level of risk (desired level).

A Risk Owner is identified for each risk.

If the target risk level is lower than residual risk, risk mitigation plans and those responsible for their implementation and deadlines shall be developed. The execution of a mitigation plan is monitored by the Risk Manager. In the self-assessment process, the findings from the assessment of risks identified are matched against the established criteria of materiality of the consequences from the relevant risks in order for the Exchange to recognise such risks as material, as well as against the established value of the risk limit (acceptable risk level).

Self-Assessment involves assessing the performance of control procedures.

Participants in the Self-Assessment assess each risk and fill in a self-assessment form.

A Risk Manager collects and systematises the results of the Self-Assessment: the presence of the same risk affecting different business units is identified, the results of the Self-Assessment are also checked against the size of total risk limit, etc.

After collecting the information in the Self-Assessment, a Risk Manager analyses the risks identified in the Self-Assessment based on the existing control procedures and remaining risk. The Risk Manager generates a list of the risks identified in the Self-Assessment for which corrective actions should be prioritised and submits them to a Business Owner for decision on risk response.

For risks, the following response choices are possible:

- risk acceptance;
- risk avoidance/elimination (in particular, the activity in question is suspended);
- risk transfer;
- risk mitigation.

In most cases a risk mitigation decision is made based on corrective actions that are developed by the responsible divisions together with a Risk Manager. The development of risk mitigation measures includes the following information:

- name of responsible employees;
- implementation period;
- marking of the activity as a project or a strategic initiative, modification or release number, if applicable.
- Further risk management is based on the procedures described in the internal operational risk management documents. A decision to respond to risk is made by a Business Owner based on assessment of the implementation costs for new controls and/or process changes and assessment of resulting benefits.

After the meetings, a Risk Manager produces Risk Maps and has them agreed by email with the heads of business units. A Risk Map is generated from the Self-Assessment template and is determined by a Risk Manager.

If a self-assessment procedure is completed in absentee format (questionnaires), the Risk Cards from the previous self-assessment are updated and agreed by email with the unit heads.

Risks identified during the Self-Assessment and those identified off-schedule, i.e. as resulting from incidents, changes in business processes, legislation, during the implementation of projects or initiatives, as a result of scenario analysis and stress testing, external and internal audits, and from risk information assessment are recorded in the risk register, which is stored in the risk database.

The procedure for documenting findings of self-assessment is as follows:

- A responsible employee of DoORIS&BC lists the risks identified in the course of self-assessment in a Self-Assessment Risk Matrix.
- A responsible employee of DoORIS&BC prepares a self-assessment report that contains a consolidated risk register, a risk map, and a summary of analytical information on the implementation of the measures for the risks identified in the previous self-assessment.
- Reports or extracts thereof may be submitted to governing bodies of the Exchange on request.

20 The procedure and frequency (at least once every six months) of test work (testing) of trading tools in accordance with paragraph 1 of Annex 1 to the Regulation on Organised Trading Activities, as well as the procedure for addressing deficiencies identified as a result of such testing

Stress tests on software and hardware facilities used for organising trades are also used to detect (identify), analyse and assess operational risks. Stress-testing frequency is determined by Exchange's internal documents, but it shall be performed at least once every six months.

Tests on organised trading tools are performed through simulation of the technical environment of organised trading in real life and, if necessary, through a test-run.

Mandatory stress-testing scenarios include:

- increasing the peak load of the components being tested by at least 50% of the maximum values for the past 6 months;
- increasing the average load by at least 30% of the average load indicators for the past 6 months
- increasing the scope of processed data by at least 30% of the average daily values for the past 6 months.

Load testing procedures:

- select a load testing environment;
- define parameters for load testing based on historical peak load values over the previous 52 weeks;
- agree on a date for load testing with trading members;
- Creating a load on Exchange's systems with an above-average load.

Load testing is performed at least once a year with trading members and for each TCS release without trading members' participation.

The Exchange shall ensure that the following operational risk management activities are implemented:

- Correction of deficiencies in the operation of the trading tools identified through tests on the trading tools;

- If critical deficiencies, including information protection vulnerabilities in trading tools (their releases), are discovered during the test work (testing) on trading tools, the tools (their releases) shall not be put into operation until these deficiencies have been corrected or the software and/or equipment has been replaced. The Trade Organiser ensures several levels of control over the reliability of its software and equipment.

The Exchange ensures several levels of control over the reliability of its software and equipment. It includes, but is not limited to, the structural units tasked with testing new or upgraded functionality, equipment upgrades and the interaction of the various components of the single suite of trading facilities, and the Change Committee. No changes to the

trading, clearing and support systems can be made unless authorised by the Change Committee.

Procedures in performing a penetration test:

- Penetration test is performed at least once a year;
- Steps to take in performing a penetration test:
  - development of terms of reference (specifications) for the job;
  - development of a threat model for the information system and software under examination;
  - software source code analysis;
  - comprehensive security analysis on information systems. The methodologies used to accomplish the specified work shall comply, without limitation, with OSSTMM, NIST, PTES, and OWASP methodologies;
  - Simulation of attacker actions targeted at achieving information security breach objectives (related to information confidentiality and integrity violation, service accessibility breach, non-repudiation breach, business logic breach) through weaknesses and vulnerabilities in information systems;
  - Checking whether previously identified vulnerabilities in Exchange's information systems have been corrected;
  - information security risk assessment;
  - development of recommendations to mitigate the identified information security risks.

DR testing procedure:

- DR testing is performed at least once a year;
- The Department of Trading and Support System Management (DoT&SSM)
- DoT&SSM and DoORIS&BC arranges and performs testing in accordance with an agreed testing plan;
- Based on the results of testing, DoORIS&BC produces a report, which should be agreed on with the internal participants in the testing;

- An action plan is developed for the gaps identified during the test, which includes particular activities, a deadline for their implementation and the people responsible for their implementation.

21 Procedure to assesses risk management efficiency by analysing Trade Organiser's performance in identifying breaches of risk limitations, correcting them and (or) implementing other measures as part of mitigating or avoiding these risks

As part of risk management process, the efficiency of risk management is assessed at least once a year by analysing the performance, quality, speed and adequacy of measures to identify breaches of risk limitations, their correction and/or implementation of other measures as part of risk mitigation or risk avoidance.

Procedure for the risk management system performance assessment;

- Set targets for the risk management system's effectiveness at the beginning of the period under assessment for the subsequent evaluation;
- Performance assessment, which involves providing an expert opinion by the Director of DoORIS&BC, including the relation between the results achieved and the resources spent on implementing risk management tools and mitigation measures, as well as assessing the quality and timeliness for addressing breaches of targets, if any, which is assessed in qualitative and quantitative metrics;
- Assess whether the current performance of the risk management system is consistent with the indicators set at the beginning of the reporting period;
- If the set indicators have been achieved, the risk management system is considered to be effective;
- The performance assessment is included in the regular risk reporting for the relevant quarter to the Executive Board and to the Risk Committee.

In addition, the KPI system includes metrics on the implementation of risk impact measures and their effectiveness, and to facilitate a more objective analysis the availability of resources allocated to these measures is also factored.

The Exchange regularly assesses risk management efficiency by analysing performance in identifying breaches of risk limitations, correcting them and/or implementing other measures as part of mitigating or avoiding these risks. The risk management system implemented and maintained by the Exchange should be assessed for effectiveness and efficiency at least once a year.

The efficiency of the risk management system is also assessed by the IAS as a business unit structurally independent of risk management business units (in particular, DoORIS&BC) at least once a year.

Risk management system efficiency is analysed based on analysis of performance in identifying breaches of risk limitations, correcting them and/or implementing other measures as part of mitigating or avoiding these risks.

A variety of existing assessment methods with prescribed performance criteria can be chosen to analyse risk management performance within the current risk management framework. The choice of assessment methods and thresholds for the assessment within a certain period of the risk management system shall be approved by the management body of the Exchange. DoORIS&BC employees collect data, analyse performance and submits data for reporting.

The risk management system effectiveness and efficiency in the Exchange is understood to be the ability of the system to achieve the following objectives and goals:

- absence of substantial losses affecting capital adequacy and the achievement of strategic objectives;
- absence of risk appetite violation records;
- compliance with the limits and restrictions set in the risk management framework;
- timely implementation of risk management recommendations delivered by IAS and external auditors;
- timely and successful test works (testing) on trading tools;
- successful testing on BC&R Plan.
- assessment of the completeness, accuracy and correctness of information in OREDB;

- assessment of the correct identification of the type and amount of losses caused by risk events (in particular, operational risk);
- assessment of the correct evaluation of the amount of losses caused by the risk (in particular, operational risk);
- assessment of the completeness and quality of measures aimed at risk mitigation (in particular, operational risk).

22 Procedure for the Exchange to take measures to prevent and manage conflicts of interest arising for the Exchange in connection with combining its activities with other activities

A conflict of interest management system shall be established for avoiding conflicts of interest, based on the following principles:

- Ensuring structural and (or) functional independence of Exchanges employees, including the heads of business units set up to carry out activities of the Financial Platform Operator and activities of the Trade Organiser/ Digital Financial Assets Exchange Operator, if the absence of the said organisational and/or functional independence leads or may lead to a conflict of interest;
- restriction on and/or control over information exchange between Exchange's employees and other persons, if this exchange of information leads or may lead to a conflict of interest
- ensuring that the remuneration systems for employees of the Exchange and to persons acting on the Exchange's account, do not allow for conditions that give rise to or may give rise to a conflict of interest;
- ensuring control over actions of the Exchange's employees and persons acting on the Exchange's account, if such actions lead or may lead to a conflict of interest;
- providing uses of financial services and customers with information about their risks arising from conflicts of interest;
- restrictions on carrying out (directly or indirectly) transactions for their own account, where the customer's proprietary information that has become known to Exchange's employees and that may pose a negative impact on the interests and rights of users of financial services is used, as well as disclosing the said information to third parties;

- informing financial services users and customers about combined activities, and the existence, in this regard, of the risk of a conflict of interest, including by disclosing information on the Exchange's website;
- implementation of double control practices (adherence to a four-eye principle);
- identifying potential risks of conflicts of interest in hiring employees who may have a conflict of interest, and setting appropriate requirements for the personal, professional and reputational qualities of candidates;
- mandatory disclosure of existing or potential conflicts of interest;
- individually address each conflict of interest, assess risks and take measures to address such conflicts of interest;
- confidentiality of conflicts of interest disclosure and their management process;
- observing the balance of interests of the Exchange and its employees in managing conflicts of interest.

In order to manage this type of risk, regular assessment procedures is performed at least once a year in order to identify other risks associated with combining the activities of the Financial Platform Operator with other activities, the identified risks shall be treated in accordance with these Rules.

23 Procedure for development and approval of the Business Continuity Plan

The Business Continuity Plan (hereinafter, the Plan) is developed by the DoORIS&BC team and the Business Units Heads concerned. The Plan shall be approved by the Supervisory Board. The Plan shall be revised at least once a year and in the event of significant changes in the Exchange’s infrastructure (emergence of new offices, changing/moving more than 20% of the workforce, etc.).

The Plan is subject to testing at least once a year. The plan shall be activated upon detection of significant incidents representing a potential threat to activities of the Exchange. The level of danger shall be determined based on incident analysis and may cause the following to be done:

- deciding on incident handling on a routine basis;
- activation of TRP for Exchange’s systems;
- activation of BCA&R plans;

- declaration of state of emergency.

When assessing the level of risk, the following definitions shall apply:

- Loss of object (office or data centre) means irretrievable loss (fire, destruction, etc.) resulting in the need to equip a new object;
- Inaccessibility of object/office means employees' temporary inability to access (due to actions of law enforcement agencies, emergencies, etc.), total absence of communication (either by main or backup channels), or failure of engineering systems (including guaranteed power supply), which leads to inability of object operation. Office means any of the key offices of the Exchange;
- Loss of IT services means unavailability of key IT systems. Example: inaccessibility of main and auxiliary trading and clearing systems of the Group;
- Loss of personnel means mass unavailability of key employees. Examples: epidemics, inaccessibility of public transport in the area of office location and so on.

24 The manner and frequency for evaluating the business continuity plan to determine whether the measures contained therein are sufficient to ensure the continuity of trade organising activities, and procedures to revise the business continuity plan if the measures contained therein are found to be insufficient to ensure the continuity of trade organising activities

The Business Continuity Plan assessment involves the following activities:

- revising the Business Continuity Plan for relevance on an annual basis, also in the event of significant changes in the Exchange's infrastructure (emergence of new offices, changing/moving more than 20% of the workforce, etc.).
- introducing changes and comments received as part of business impact analysis from the Exchange's business units;
- getting a new version of the Business Continuity Plan by all business units involved and approval from an authorised collegiate body.

25 Procedure for identifying emergencies and analysing the circumstances in which they occur

Emergency and abnormal situation management involves emergency and abnormal situation detection procedures, decision-making in an emergency or in an abnormal situation, communication procedures, recovery and consequence management procedures.

Managing business continuity risks entails defining objectives, targets, procedure, methods and timing of the set of measures on prevention or joint elimination of the consequences of possible violation of day-to-day functioning of the Exchange (its business units) caused by unforeseen circumstances (occurrence of emergency situation or other event that is likely to happen, but hardly to predict and relates to a threat of material financial losses or other consequences preventing the Exchange from fulfilling assumed obligations), describing operational processes and prioritising activities of the Exchange from the announcement of an emergency till the moment when normal operations are resumed and the emergency is then cancelled, based on the worst-case scenario (main office is unavailable; primary data centre is unavailable; main office and primary data centre are unavailable).

The Exchange ensures that the following efforts are implemented:

- Identification of emergencies and analysis of the circumstances in which emergencies occur. The process is regulated by internal documents on operational risk and business continuity;
- Keeping the back-up office at the level that ensures the possibility of functioning of all critical processes of the Exchange and maintaining such processes for at least one month from the emergency event occurrence

Identification of emergencies and analysis of the circumstances in which they occur is an important part of the Exchange's risk management system.

26 Procedure for maintaining a list of potential emergencies by the Exchange

Procedures for maintaining a list of potential emergencies include the following:

- identifying the areas that may expose the Exchange to business continuity risks;

- identifying potential emergencies that may lead to disruption of critical processes identified throughout the business impact analysis;
- analysing effects from potential emergencies on the Exchange should they occur, including:
  - employees of the Exchange;
  - trading facilities of the Exchange;
  - Exchange's infrastructure;
  - effect on assessment of the likelihood of a threat;
  - effect on analysis of existing control procedures;
  - effect on identification of possible risk minimisation measures.

27 Procedure for distributing responsibilities and authorities between business units of the Exchange and their employees in the event of material operational risk event.

The procedure for distributing responsibilities and authorities between business units of the Exchange and their employees in the event of material operational risk events involves the following:

- When a material operational risk event (abnormal situation) occurs, the Working Group of the Moscow Exchange Group employees meets. They perform an initial assessment of the event, decide on actions to be taken in a specific situation and/or on convening an Extended Working Group comprising members of the Executive Board, and coordinates the actions of Moscow Exchange Group companies to address abnormal situations; In case of an emergency change in the established limits, the Exchange shall act in accordance with the Regulations for Moscow Exchange, NCC, NSD and NAMEX Business Units in Emergency Situations During Trading and Clearing;
- Any employee discovering an abnormal situation or evidences that a situation is abnormal, is obliged to report it to a member of the Working Group;
- A member of the Working Group receiving information about an abnormal accident must immediately start clarifying the nature of possible cause and consequences of the accident;

- An occurred abnormal situation is analysed, and the measures necessary for decision-making on response actions, including suspension of trading, closure of trading, changes in trading, clearing and/or settlement times in accordance with the trading and/or clearing rules, as well as measures for notifying participants, regulators and counterparties of the consequences are determined;
- Monitoring the implementation of measures to be taken to mitigate the consequences of abnormal situation.
- The Exchange's press service regularly notifies trading/clearing members of abnormal situations and the measures taken by Moscow Exchange Group companies to address the consequences of such situations (via Moscow Exchange's official website and/or in the media). After 6 p.m., a notice may be given by employees of the Operations Department (on Moscow Exchange's official website);
- If an abnormal situation causes suspension of trading, a member of the Working Group immediately reports it to the Duty Operations Director. The Duty Operations Director promptly organises and, no later than 15 minutes after an abnormal situation is discovered, ensures that information about it is disclosed on Moscow Exchange's official website;
- The Duty Operations Director coordinates employees of Moscow Exchange in order to:
  - send a message of abnormal situation to trading members, management, the Bank of Russia and vendors via PNS;
  - notify the Bank of Russia
  - convene a meeting of the Extended Working Group.

- If an occurred abnormal situation does not result in a suspension of trading, a member of the Working Group notifies all the members of the Working Group on a conference call.

- A member of the Working Group receiving the information about abnormal situations reports the following:
  - time of receiving information of a NRS;
  - employee reporting a NRS;
  - causes and consequences of a NRS.

Members of the Working Group work out a collegial decision regarding actions to address an abnormal situation:

- If a decision is taken to suspend trading, such suspension takes place no later than fifteen minutes after a failure is detected;
- When deciding that the Working Group meets in an extended format, the Duty Operations Director arranges the work in accordance with the following procedure:
  - The Duty Operations Director coordinates on the overall organisation and work of the Extended Working Group;
  - To organise the work of the Extended Working Group, the Duty Operations Director informs the members of the Extended Working Group and ensures that a conference is organised to hold the meeting.

Once the causes of the event have been eliminated and/or the normal functioning of software and hardware has been resumed, the Duty Operations Director ensures that:

- information on the time the trading system becomes available for withdrawal of orders, resumption time and trading procedures is disclosed on the Moscow Exchange's official website no later than 15 minutes before trading resumes. Information is disclosed on Moscow Exchange's official website on the Internet by OD employees;
- Messages to trading members, Moscow Exchange Group management, as well as to the Bank of Russia and vendors about the resumption time and trading rules are sent via PNS. PNS messages are sent by employees of Operations Department;
- Notices on the resumption time and trading procedures are sent to the Bank of Russia. Messages to the Bank of Russia are sent by ICS employees;
- A Bank of Russia’s representative is notified of trading resumption and trading regulation;
- Organisations that have entered into cooperation agreements with Moscow Exchange in relation to lending and deposit transactions are notified of the time when deposit transactions with banks resume;
- If it is necessary to reschedule other routine operations that may affect trading members, the Moscow Exchange Group company concerned discloses a notice on

rescheduling routine operations on its official website, unless such notice cannot be given due to a technical failure;

- Information is shared to mass media and media relations are established;
- Once a material operational risk event occurs, DoORIS&BC arranges for the development of an action plan to manage the event and mitigate the negative consequences thereof jointly with responsible business units, and arranges for the development of an action plan to prevent such event in the future, indicating the deadlines and those responsible for the implementation of the action plan;
- DoORIS&BC monitors compliance with the time requirements and implementation of action plans referred to above and may also develop key risk indicators for monitoring the level of risk associated with a material operational risk event occurred;
- If a material operational risk event has resulted in a breach of defined risk appetite thresholds, the information is escalated and reported to the Executive Board, the Risk Committee at the Supervisory Board and the Supervisory Board.

28 Procedure for the Risk Management Rules assessment

The Exchange assesses the Risk Management Rules as and when necessary (but at least once a year) for their relevance and effectiveness and, if any irrelevant information and (or) measures are identified in them that, in the Exchange's opinion, do not ensure the effectiveness of the risk management system, revises these Rules.