APPROVED

by the resolution of the Supervisory Board

of Moscow Exchange

on August 1, 2025

Minutes No. 4

Business Continuity Management Policy of Public Joint-Stock Company “Moscow Exchange MICEX-RTS”

Table of Contents

Revision Sheet

Version No.	Date of approval	Description	Authored by
1	28 February 2017	Initial version approved by the Supervisory Board of the Moscow Exchange	S.V. Demidov
2	26 February 2018	Approved by the Supervisory Board of Moscow Exchange as amended	S.V. Demidov
3	7 October 2021	Approved by the Supervisory Board of Moscow Exchange as amended	S.V. Demidov
4	4 December 2023	Approved by the Supervisory Board of Moscow Exchange as amended	S.V. Demidov
5	25 September 2024	Approved by the Supervisory Board of Moscow Exchange as amended	S.V. Demidov
6	1 August 2025	Approved by the Supervisory Board of Moscow Exchange as amended	S.V. Demidov

Definitions and Abbreviations Used. Related Documents

The terms not specifically defined herein shall be used within the meanings specified in internal documents of Moscow Exchange Group, as well as by the laws and regulations of the Russian Federation.

Table 1-1. Terms, Definitions and Abbreviations

Term	Definition
Index Administrator	The Exchange that is registered with the Bank of Russia as an Index Administrator and operates under the Federal Law No. 452-FZ About Administrators of Financial and Commodity Indices dated 13 December 2024 and related regulatory acts.
Assets	Resources controlled by the Exchange based on the results of past events, the use of which may lead to economic benefits in the future (tangible and intangible assets).
Business Impact Analysis (BIA)	A structured process for measuring the consequences of Exchange's business processes interruptions in both quantitative (financial) and qualitative (non-financial) aspects over a period of time and to determine the resources required to implement them in the event of an abnormal and/or emergency situation.
BCMS Audit	Systematic, independent and documented process of BCMS objective assessment to determine the degree of the established tasks implementation (audit criteria).
Exchange	Moscow Exchange
Primary Emergency Response Centre, PERC	Primary Emergency Response Centre, PERC is a working body of the Exchange authorised to make decisions on issues related to the occurrence of abnormal situations during trading and in the course of Financial Platform Operator's activities, activities of Exchange Operator. The PERC also develops recommendations to the authorised bodies of other companies of Moscow Exchange Group on the abnormal situation settlement issues during trading and clearing and in the course of activities of the Exchange Operator and Financial Platform Operator's activities.
Management of the Exchange	Exchange Executive Bodies
Documented Information	Information that is submitted and maintained by the responsible departments and (or) persons of the organisation. Documented information could be in any format, including electronic.
Stakeholder	Individual and (or) legal entity (or set of people), organisation that may be affected by decisions/results of the Exchange activities.
Incident	A situation that might constitute an interruption of normal operations, loss, emergency, crisis, or lead to occurrence of the same. The reason may be: disruption of normal operation of critical software and hardware tools supporting critical processes of the Exchange; disruption of the Exchange critical processes; inoperability (inaccessibility) of the main communication channels, including the Exchange corporate network, the Internet network, other communication channels with the interacting organisations, which are required to implement the Exchange critical processes; inability of the Exchange employees to be physically present at their workplaces due to fire, floods, accidents, acts of terror, diversion, sabotage, natural disasters and other circumstances of insuperable force; other cases which may lead to disruption of the Exchange normal operation.

Term	Definition
Exchange Executive Bodies	The Executive Board of the Exchange and (or) the Chairman of the Executive Board (CEO) exercising operational management activities in accordance with the Exchange's Charter.
Recovery Teams	Teams built up out of employees of division, which are engaged once the emergency occurs. Employees directly involved in recovery of Exchange's operations (process recovery) and/or ensure continuity of the same. The activities of Recovery Teams are regulated by BCR plans of structural divisions.
Emergency Control Command Centre	Location of Primary Emergency Recovery Centre members equipped with necessary materials and technical resources. For information confidentiality reasons, the Emergency Control Command Centre must be isolated from the rest of the premises and locked with a key.
Critical Process	A process of the organisation which, if disrupted due to operational risk events, will result in disruption of the Exchange's operations, including technological processes that require information interaction, data processing and storage by using software and hardware tools.
Critical Software and Hardware Tools	Software and hardware tools, which, if their functioning fails, may result in disruption of critical processes
Division Business Continuity Coordinator (BC Coordinator)	One or more employees of the Division authorised to submit information in terms of their Division's BC to the BC Manager, to liaise within the framework of BC activities and procedures and to keep the Division's BCR Plan up-to-date.
Business Continuity Supervisor (BC Supervisor)	An official who supervises BC and is responsible for ensuring business continuity at the Exchange in accordance with internal and/or organisational and administrative documents of the Exchange.
Initial Emergency Response Centre, IERC	A working group consisting of employees of the Moscow Exchange Group companies, which performs initial assessment of an abnormal situation and develops recommendations in a particular abnormal situation context and/or decides on the PERC convocation. The list of IERC members is made available on the corporate internal portal's page "Our work/Handling abnormal situations" and in the Exchange BC Plan.
BC Manager	An employee of the Exchange entrusted with the tasks of operational management of the Exchange BC processes, including monitoring the implementation of policies, procedures, conflict resolution, resource mobilisation, reporting on key indicators, etc.
Non-Critical Division of the Exchange	A division of the Exchange implementing the business processes, the suspension of which within the established deadlines does not carry any risks of suspension of the Exchange principal activities (critical processes), including the fulfillment of obligations to stakeholders by the Exchange.

Term	Definition
Business Continuity	The Exchange strategic and tactical ability to plan its work in case of violations of normal operation (emergency situations) aimed at ensuring the continuity of services provisioning to clients, counterparties and other stakeholders at the established acceptable level.
Abnormal Situation	Circumstances that cause and/or lead to failures (outages) in operations of software and hardware systems and subsystems of the Exchange, Financial Platform Operator, Exchange Operator, Index Administrator and/or directly impede their normal (regular) operation, and other circumstances that may significantly affect the Exchange's normal operations, as defined in accordance with the Regulations on Abnormal Situations
Business Continuity Assurance	Assuring continuity of the Exchange's business.
Financial Platform Operator	The Exchange as a legal entity engaged in activities related to ensuring execution of financial transactions between financial institutions or issuers and consumers of financial services using a financial platform, and included by the Bank of Russia into the registry of financial platform operators. The Financial Platform Operator is not a party to financial transactions executed with the help of the financial platform.)
Exchange Operator	The Exchange included by the Bank of Russia in the registry of DFA exchange operators and acting as a CFA exchange operator, which ensures transactions conclusion by collecting and comparing multidirectional orders for such transactions, as well as settlement of transactions.
Exchange Offices	Exchange's buildings housing the main and backup workstations of Exchange employees.
Software and Hardware Complex Recovery Plan	Disaster recovery plan for the Software and Hardware Complex of the Exchange.
BC Plan	The Business Continuity Plan of Public Joint-Stock Company "Moscow Exchange MICEX-RTS" is a document that defines the basic principles of action in the event of an unusual and (or) emergency situation as well as the procedure for responding to failures and ways to resume, restore critical processes within a predetermined period at an acceptable level set.
BCR Plan of a Structural Division	A detailed plan of actions in emergencies to be followed by a Structural Division or by a Centre of Excellence of the Exchange (Business Continuity and Recovery Plan)
Exchange Division	A separate business unit of the Exchange
Risks Management Policy	Internal document of the Exchange defining the principles of risk management within the company.
Software and Hardware Complex	A set of software and hardware, such as IT systems and IT infrastructure, databases, telecommunication facilities, other equipment and software.
BCMS Processes	A set of organisational measures, procedures and resources aimed to maintain BCMS effective operation.
Employees	Employees of the Exchange working for the Exchange under an employment agreement; Citizens doing work for the Exchange under a civil law contract.

Term	Definition
Regulations on Abnormal Situations	An internal group-wide document that regulates interactions between the Moscow Exchange Group companies in the event of abnormal situations occurred during trading and clearing and in the course of Financial Platform Operator's activities. The Regulations define the ways of informing about the situation, the operations procedure in case of identification of an abnormal situation and its elimination.
Backup Office	The premises equipped with certain technical means sufficient to organise recovery and maintain Moscow Exchange operation in the event of emergencies that make it impossible for the Exchange to perform its activities in whole or in part using the premises and/or technical infrastructure of the main office.
Resources	All material and technical assets, human resources, skills, information, technology (including machinery and equipment), premises, material and technical values and information (in electronic or any other form) that the organisation must possess to use as required to carry out its activities and achieve its goals.
Risk	An event or condition that, upon occurrence, would have a negative impact on business processes, services, and clients, and that leads or may lead in potential losses that may result in loss of revenue, additional costs, or a negative impact on business reputation.
Business Continuity Management System, BCMS	Part of the overall organisation management system aimed at development, implementation, daily work, monitoring, reassessment, maintaining and improvement of business continuity.
Mixed Operation Mode	Alternating work in the office and remote work.
BCMS Improvement	Ongoing, continuous and recurring activities aimed at improving the quality of BCMS and its efficiency.
BC Testing	Activities during which actions are fully or partially completed in accordance with the BC Plan to ensure that the BC Plan(s), the BC Strategy are suitable for their implementation, relevant and consistent with the BC objectives.
Business Process Disruption Factor (Risk Factor)	A circumstance that has caused or may cause the occurrence of a risk event that may entail a disruption of the normal operation of the Exchange and (or) cause the risk of suspension of the Exchange operation.
Financial Platform	An information system that provides interaction of financial institutions or issuers with consumers of financial services (hereinafter, "participants of the financial platform") through the Internet information and telecommunication network to enable execution of financial transactions with the access thereto provided by the financial platform operator.

Term	Definition
Centre of Excellence	A functional grouping within one or more business divisions with a specific function (service) in more than one legal entity within the Moscow Exchange Group.
Digital Financial Assets (DFA)	Digital Financial Assets are digital rights, including monetary claims, enjoyment of rights to equity securities, rights to participate in the equity of a non-public joint stock company, rights to demand transfer of equity securities, which are contemplated by the decision to issue DFA, whose issue, accounting and circulation are possible only by making (changing) entries in a blockchain-based information system.
Emergency	A situation (including non-standard and (or) abnormal one) which entails disruption of routine operation of the Exchange, normal activities of its employees that is associated with the threat of significant material losses or other consequences that prevent the Exchange from fulfilling its obligations.

Table 1-2. Related Documents

Subclause No	Document name
1.	Business Continuity Strategy of Public Joint-Stock Company “Moscow Exchange MICEX-RTS”
2.	BC Plan of the Exchange
3.	Risk Management Policy of Public Joint-Stock Company “Moscow Exchange MICEX-RTS”
4.	Business Continuity Risks Assessment. Process description
5.	Business Impact Analysis. Process description
6.	Regulations on Abnormal Situations
7.	Testing of BCMS procedures. Process description
8.	Monitoring, Measurement, Analysis and Assessment of BCMS. Process description
9.	Record Keeping Manual of Public Joint-Stock Company “Moscow Exchange MICEX-RTS”
10.	Procedure for Monitoring the Orders Execution of the Chairman of the Executive Board at Public Joint-Stock Company “Moscow Exchange MICEX-RTS”
11.	Regulations for Dealing with Information Constituting Trade Secrets of Public Joint-Stock Company “Moscow Exchange MICEX-RTS”

1. General Provisions

This Policy on Business Continuity Assurance of Public Joint-Stock Company “Moscow Exchange MICEX-RTS (hereinafter referred to as the “Policy”) is a fundamental document of the business continuity management system. The Policy is designed based on the Bank of Russia Methodological Recommendations No. 28-MP dated 18 August 2016, intentional standard ISO 22301:2019 Security and Resilience - Business continuity management systems - Requirements and in line with the Exchange’s goals. The Policy establishes a set of management and organisational rules, requirements and principles on the basis of which the Exchange's business continuity management system (hereinafter and before referred to as “BCMS”) is being developed, implemented, functioning and constantly improving.

This Policy defines:

- goals and objectives of BCMS operation and its scope of application;
- organisational and role model of BCMS;
- principles of business continuity management, applicable practices and standards encompassing regulatory requirements;
- established procedures and utilised resources necessary for BCMS support and development;

- methods of mandatory continuous BCMS improvement.

This Policy is a public document, the information thereon is disclosed on the official website of the Exchange and is available for reading to all employees of the Exchange on the corporate portal.

2. Scope and Coverage

BC Policy Scope

This Policy does not impact the issues of managing political, economic and market risks as well as the risks of amendment of legislation of the Russian Federation.

This Policy is considered strictly in line with other internal documents of the Exchange. In the event of a conflict between this document and other internal documents of the Exchange that impact the issues of the BC Policy, this Policy shall have a higher priority in terms of regulating the BC processes, with the exception of the Exchange's Charter.

This Policy is a binding document to be used and enforced by all divisions of the Exchange. The Policy covers business continuity of Exchange's subdivisions operation when working, including in the Exchange's offices, when working remotely and when working in a mixed mode.

BCMS Scope and Coverage

The Exchange BCMS covers all key services offered by the Exchange, such as trade organisation services, services on the securities market, derivatives, FX and precious metals, standardised OTC derivatives, deposit and credit markets, DFA market, services of the financial platform operator, exchange operator and index administrator.

The priority of emergency planning and the scope of protective preventive measures are determined depending on the results of business continuity risks and threats assessment and business impact analysis.

The Exchange BCMS pursues the bank's mission, meets the established values and represents an instrument of Exchange's operational reliability.

The requirements, needs and expectations of the stakeholders identified in the section below shall be taken into account in building the BCMS and defining its coverage.

The Exchange is aware of the dependence of its activities on internal and external factors, problems that may immediately affect its operations and may potentially impact the ability of the Exchange to achieve its target outcomes. The exchange proactively seeks to anticipate potential internal and external factors and errors, prevent their occurrence, and identify actions that could mitigate potential consequences in the event of problems.

To obtain adequate assurance in the relevance of BCMS coverage, changes in Exchange's activities are continuously monitored. The BCMS coverage is updated as required.

3. Business Environment and Potential Opportunities

Public Joint-Stock Company "Moscow Exchange MICEX-RTS" (hereinafter and before referred to as the "Exchange") is the biggest trade organiser in Russia and it provides Russian and international professional financial market participants and its clients with a wide range of opportunities to trade shares, bonds, fund units, derivatives, currency, government securities, DFA and commodities. The Exchange organises trades on the Equity and Bond Market, Derivatives Market, FX and Precious Metals Markets, Standardised OTC Derivatives Market, Deposit and Credit Markets, DFA Market. It also provides services of the financial platform operator and index administrator.

The Exchange offers its clients information and technological services providing market data (including the values of the calculated indices) both in real time and on the basis of trade results.

The Exchange actively promotes the Russian financial market and its infrastructure, improves technologies and increases attractiveness of its trading facilities and services to organise trade in the markets for Russian and international investors and issuers.

Potential opportunities

The Exchange has the following potential opportunities ensuring achievement of expected results for BCMS:

- competent and informed employees of the Exchange receiving periodical professional training;
- a set of measures to ensure business continuity and business recovery in case of emergency is implemented and supported;
- fail-safe solutions for critical software and hardware tools of the Exchange are developed and kept in a good working order;
- necessary backup infrastructure is identified and kept in good working order;
- high transparency of the Exchange activities in compliance with the actual corporate governance standards;
- corporate governance code takes into account the best international practices.

4. Strategic Goals and Objectives of BCMS

The Exchange BCMS has the following strategic goals[1]:

- ensuring that the Exchange fulfils its obligations to its clients, counterparties and other stakeholders as defined below;
- ensuring the safety of employees and visitors located in the offices and premises of the Exchange;
- prevention of potential violations of the Exchange normal operation;
- mitigation of material and non-material consequences in cases of violation of the normal operations;
- restoration of normal operation after emergencies in compliance with the established indicators.

The main objectives of BCMS are:

- identification of threats, monitoring and continuity risk assessment, identification of emergency scenarios;
- determination of the organisational and role model of BCMS management;
- identification of critical processes and critical software and hardware tools, along with their recovery target values, taking into account the risk appetite, nature and scale of the Exchange operation;
- identification of external and internal resources required to implement critical processes, along with their recovery target values;
- development of BC strategies and decisions;
- development of measures to reduce the impact of emergencies and advance planning of recovery activities in case of emergencies;
- maintaining the level of management of the Exchange in the emergency context, which allows to ensure the adoption of reasonable and adequate management decisions, their timely implementation;
- ensuring the compliance of BC procedures and documents with regulatory requirements;
- preparation of the Exchange employees to act in abnormal situations, provision of recommendations and assistance to the Exchange employees in the field of BC (including regular training events).

The Exchange stakeholders include:

- the Central Bank of the Russian Federation (the Bank of Russia), state bodies regulating the activities of the Exchange in the relevant areas and imposing regulatory requirements in terms of BCMS;
- issuers, clients and counterparties of the Exchange expecting uninterrupted provision of services;
- shareholders of the Exchange who expect the Exchange to fulfil its obligations at a high level that provides a competitive advantage and meets the needs and expectations of its clients;

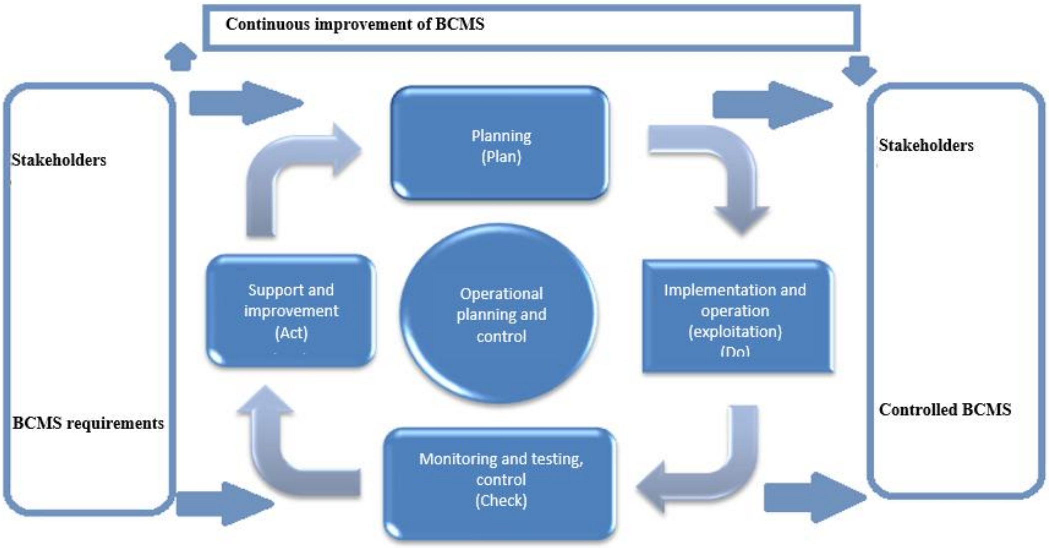
[1] The detailed objectives of BCMS for the planned period are established during BCMS planning procedure, the description of which is provided in Chapter 9 of this Policy.

- internal users – employees of structural divisions directly involved in the Exchange's activities.

5. Life Cycle of the BCMS

BCMS lifecycle is fundamental for the efficient operation of the business continuity management system. BCMS lifecycle is built in accordance with the recommendations of ISO 22301:2019, with the Deming cycle (PDCA[2]) – planning, implementation and operation, monitoring and testing, support and continuous improvement.

Effective BCMS: cyclic, interrelated between the principle activities of the divisions and the operation recovery activities.



While implementing the stages of BCMS lifecycle, the following tasks shall be resolved:

Planning (Plan): analysis of existing threats and potential emergency effects for business, development of the BC Policy and Strategy, definition of BCMS goals and objectives, design of processes and procedures to ensure business continuity, establishment of BCMS control and management points.

Implementation and operation (Do). Business continuity planning in accordance with the selected strategy: development of divisional BCR Plans and Recovery Plans for Software and Hardware Complex, development of employee training programs, creation of the necessary backup infrastructure, determination of the procedure for its use.

Monitoring and Testing (Check). Activities on the regular conduct of tabletop exercises and testing of the Plans and parts thereof, monitoring of business continuity procedures, preparation and submission of the assessment results of BCMS efficiency.

Maintaining and continuous improvement (Act). Development and application of corrective measures based on the results of tests, exercises, audits and assessments of BCMS efficiency as well as initiating a review of the scope, objectives, tasks and resources of BCMS. Improvement of BCMS quality, consideration and accounting of BCMS best practices.

Operational planning and control. These should be performed throughout BCMS life cycle and includes development and implementation of this Policy, definition and management of BCMS organisational structure (roles and responsibilities), definition and implementation of measures for management and business continuity management, management of the program for the implementation of BC processes and the development of BCMS structure.

[2] PDCA – PDCA cycle (Plan, Do, Check, Act)

6. BCMS Documentation

Regulatory documents governing BCMS of the Exchange[3]:

Regulatory document	Type of control
Federal Law No. 325-FZ, dated 21 November 2011, "On Organised Trading"	Requirement for BCMS accounting
Federal Law No. 39-FZ, dated 20 April 1996. "On the Securities Market"	Requirements for BCMS accounting
Federal Law No. 211-FZ, dated 20 July 2020 "On Execution of Financial Transactions Using Financial Platforms"	Requirement for BCMS accounting
Federal Law No. 259-FZ, dated 31 July 2020, "On Digital Financial Assets, Digital Currency and on Amendments to Certain Legislative Acts of the Russian Federation"	Requirement for BCMS accounting
Federal Law No. 452-FZ About Administrators of Financial and Commodity Indices dated 13 December 2024 and related regulatory acts.	Requirement for BCMS accounting
Federal Law No.69-FZ, dated 21/12/1994, "On Fire Safety"	Requirement
Federal Law No. 68-FZ, dated 21 December 1994, "On Protection of Population and Territories from Natural and Man-made Emergencies"	Requirement
Resolution of the Government of the Russian Federation No. 304, dated May 21, 2007, "On the Classification of Natural and Man-made Emergencies"	Requirement
Decree of the Government of Moscow No. 124-PP, dated 24 February 2009, "On the Organisation of Emergency Prevention and Response Planning"	Requirement
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"	Requirement for BCMS accounting
Bank of Russia Methodological Recommendations on Ensuring Uninterrupted Operation of Non-Bank Financial Institutions, No. 28-MR, dated 18 August 2016	Requirement
Bank of Russia No. 779-P, dated 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)"	Requirement for BCMS accounting
Russian National Standards of the GOST R 53647 family of "Business continuity management"	Requirement
ISO 22301:2019 (Security and Resilience - Business continuity management systems – Requirements)	Requirement for BCMS accounting

Internal documents on BCMS

Key internal documents on BCSM	Approval
1. BC Policy 2. BC Plan	Supervisory Board of Moscow Exchange
3. BC Strategy 4. Business Continuity Risk and Threat Assessment. Process description 5. Business Impact Analysis. Process description	Exchange Executive Bodies

[3]Regulatory documents are valid at the time of approval of the Policy. When changes are made to the documents listed above, these documents will be deemed to be valid and/or consistent with the new titles and versions.

Key internal documents on BCSM	Approval
6. Monitoring, Measurement, Analysis and Assessment of BCMS. Process description; 7. BCMS Testing. Process description 8. Management's analysis BCMS (report) 9. Business continuity threat map 10. Report on the results of the Business Impact Analysis 11. BC Plan Test Program 12. Report on the results of the BC Plan testing	
13. Regulatory testing results	BC responsible employee (BC Supervisor)
14. Division's BCR Plan	Division Head
15. Software and Hardware Complex Recovery Plan	Working document approved by the Heads of responsible IT divisions and the persons in charge of BCMS
16. Regulations on Abnormal Situations	Exchange Executive Board

The above list of internal BCMS documents is not exhaustive. If necessary, other internal BCSM documents may be developed in addition based on the requirements of this Policy and regulatory and normative requirements on BC.

Document Management Process

The BC Manager continuously monitors regulatory documents in terms of applicable BCMS recommendations and requirements maintain compliance with new requirements and continuous BCBS improvement.

In order to track new legislative, regulatory and other documents related relevant for the BC activities of the Exchange, as well as to streamline the process of developing internal documents and materials, the Exchange has a document management process in place.

7. BCMS Management Model: Roles and Responsibilities

The Exchange has in place a distributed business continuity management role model that meets the goals and objectives of BCMS and ensures the efficiency of its work. The management role model falls into the normal operation and emergency modes.

If necessary, additional roles may be defined as well as detailed instructions for the roles envisaged in this Policy. Supplement to this organisational and role model shall be approved by the Exchange Supervisory Board.

Roles and areas of responsibility in the daily operation mode:

In the daily operation mode of the Exchange, the common tasks at all levels of BCMS management shall be to develop and support BCSM management processes, infrastructure and mechanisms.

Role/Management Body	Description
Business Continuity Supervisor (BC Supervisor)	An official who supervises BC and is responsible for ensuring business continuity at the Exchange in accordance with internal and/or organisational and administrative documents of the Exchange. Area of responsibility: • management of BC processes, including definition of the main areas of BC, coordination of BC processes; • making decisions to support and improve BCMS; • provision of the resources for the implementation of measures to support and improve BCMS; • coordination and submission for approval documentation in the field of BC; • monitoring the implementation of the Policy's provisions and other internal documents governing BCMS operation;

Role/Management Body	Description
	• coordination and monitoring of implementation of testing, training and awareness raising programs for the employees in the field of BC; • reporting on BCMS performance to the Executive Bodies of the Exchange etc.
Business Continuity Manager (BC Manager)	One or more employees of the Department of Operational Risks, Information Security and Business Continuity of the Exchange with job responsibilities involving business continuity assurance functions. Area of responsibility: • strategic planning and implementation of BCMS development plans; • preparation of proposals on BCMS support and development budget; • organisation and coordination of BCMS support and development; • development and revision of BCMS document support; • development of BC Strategy proposals; • organisation and conduct of business continuity risks and threats assessment; • organisation and performance of Business Impact Analysis; • support, control and methodological support to Division BC Coordinators; • arrangement and coordination of activities to raise awareness of the employees in the field of BC; • organisation and coordination of BCMS monitoring and testing; • preparation and submission of reports for the management (including proposals for eliminating shortcomings identified in BCMS testing); • methodological and export support to Divisions on BC matters.
Division Business Continuity Coordinator (BC Coordinator)	One or more employees of the Division authorised to submit information in terms of their Division's BC to the BC Manager, to liaise within the framework of BC activities and procedures and to keep the Division's BCR Plan up-to-date. The required number of Coordinators shall be determined/appointed by the Division Head (in electronic form). The role is offered to an employee with sufficient experience and overall understanding of all the activities of the Division. Area of responsibility: • collecting data on the Division's activities and completing the Business Impact Analysis form for their Division, participating and engaging other employees in their Division in interviews for the purpose of the Business Impact Analysis; • organisation or participation in BCMS testing, preparation and submission of reporting materials and data analysis based on the results of testing to the BC Manager; • pro-active participation in the development of the Division's BCR Plan (supported methodologically by the BC Manager); • monitoring of changes in the Division and transfer of data to the BC Manager (personnel, functional, process, technological, resource), requiring revision of the Division BCR Plan; • revision and update of the Division BCR Plan, agreement on the updates with the BC Manager and the Division Head.
Division Head	Head of Exchange Division according to the staffing table. Owner of the Division BCR Plan. Area of responsibility: • appointment of the BC Coordinator(s) of the relevant Division and overall supervision of their activities; • allocation of the required resources for participation of the Division in BC activities (including testing of BCMS and raising the awareness of its employees in the field of BC); • conducting business impact analyses in their Division, identifying resource requirements to ensure business continuity for the Division;

Role/Management Body	Description
	• approval of the results of the Business Impact Analysis and the results of revision (updating) of the BCR Plans as related to their respective Division); • ensuring compliance with the BC requirements by the employees of their Division and (if applicable) third parties with whom interaction is carried out within the frameworks of official duties (by including, inter alia, these requirements into contracts, agreements with third parties); • keeping the BCR Plan of the relevant Division up to date.
Division Employees	All employees in the Division. Area of responsibility: • familiarisation with BCMS internal documents; • timely completion of mandatory BCMS training courses; • participation in BC activities and procedures in the part related to the Division; • compliance with the BC requirements of the Division and the Exchange.
Non-Financial Risk and Information Security Management Committee of Moscow Exchange	The advisory body of the Exchange regulated by the Regulation on the Committee for Management of Non-Financial Risks and Information Security.
Exchange Executive Bodies	The Exchange Executive Board and/or Chairman of the Exchange Executive Board (the sole executive body). Area of responsibility: • operational management of the Exchange in accordance with the its Charter.

Roles and areas of responsibility in the emergency mode

In the emergency mode, the common task across all levels of BCMS management models is to minimise the consequences of the emergency and resume normal operation of the Exchange as soon as possible.

Role/Management Body	Area of responsibility
BC Supervisor	• Coordination of PERC activities: initiation, organisation and keeping records.
Initial Emergency Response Centre (IERC)	• Determination of the degree of impact of emergency situations on the Exchange activities, assessment of the damage caused as a result of emergency situations; • Decision-making on notification of stakeholders; • Decision-making on the convocation of the PERC.
PERC – Primary Emergency Response Centre.	• Development of recommendations to the Exchange's executive bodies on switching to emergency operation, managing the Exchange in the emergency mode, returning to normal operations and ending the emergency mode; • Coordination of restart of critical processes and interactions with law enforcement authorities, emergency and specialised services, utilities, and ensuring that necessary support is provided to Exchange employees and their family members;
Recovery Teams	• Implementation of activities in accordance with the BCR Plans; • Ensuring operation of critical processes in the team's area of responsibility; • Restoration of technical and resource conditions for the Resumption of critical processes (including activation of the backup office); • Rehabilitation of infrastructure (offices and hardware-software complex).
Business Continuity Manager (BC Manager)	• Overall coordination of the Exchange employees in accordance with the BC Plan or BCR Plans of the divisions; • General coordination and implementation of internal communications; • Methodological support on the issues of activity recovery; • Recording the results of restoration of technical, administrative and business functions for subsequent analysis and potential BCMS improvement.

Role/Management Body	Area of responsibility
Exchange Employees	The Exchange employees act in accordance with the requirements of the instructions for actions in emergency situations; the BC Plan, the Divisions' BCR plans and current recommendations of the managers.
Security Service, Business Department	• Providing conditions for the early evacuation of people located in the Exchange office(s), as well as the Exchange property, if necessary; • Interaction with the headquarters and emergency services formed by municipal and (or) federal state bodies; • Protection of assembly points for the Exchange employees and stockpiling of the Exchange property in case of evacuation of people and property; • Interaction and provision of unhindered access to the Exchange office (s) by municipal and/or federal emergency services, if necessary; • Ensuring prompt access of the Exchange employees involved in the implementation of the BCR Plan(s) at the backup sites.
Heads of Divisions	• Managing and supervising the Divisions' employees in activities in accordance with the accepted BC Strategy and Plan; • Reporting on the implemented measures while recovering the unit's operations, etc.
Exchange Executive Bodies	Operational management of the Exchange, including in the emergency mode, making decisions related to strategy under implementation based on the opinion of the PERC. Exchange Executive Bodies' Responsibility is established in accordance with the legislation of the Russian Federation.

Participation of the Exchange Executive Bodies in BCMS

Participation of the Exchange Executive Bodies in the BC process is of crucial importance. In particular, the Exchange Executive Bodies take part in such issues as:

- support for regulatory requirements, resource and financial obligations;
- determining the priority of BC among other (strategic) business operations and initiatives of the Exchange;
- integration of BCMS into all other business areas of the Exchange in connection with the management and development of the Exchange;
- demonstrating to the rest of the employees the importance of the role played by BCMS in the activities of the Exchange.

Fulfilment of BC obligations in terms of the Exchange Executive Bodies and confirmation of their involvement are demonstrated through BCMS documents approval, the appointment of persons responsible for BCMS and the allocation of responsibilities, the provision of necessary resources and financial means, as well as active participation and expression of interest, regular analysis of BCMS.

In view of the need for a deep understanding of business processes and specifics of business while planning the business continuity, BCMS uses a matrix approach to governance under which the responsibility for ensuring the continuity of critical processes is assigned, among other things, to the heads of independent divisions of the Exchange (the owners or executors of which they are).

8. BCMS Activity Planning

BCMS activity planning includes:

- setting BCMS goals taking into account changes in the context of the organisation (if applicable) and expectations of the stakeholders (if applicable);
- planning the procedures and (or) ways to achieve the intended goals (in particular, list of resources uses; responsible employees; estimated deadlines; descriptions or metrics for assessing the procedures' results);

- determining risk mitigation efforts and their implementation controls;
- planning of BCMS changes taking into account best practices and the intent for continuous BCMS improvement.

When planning BCMS goals, it is necessary to take into account that the goals must: comply with the BC Policy; be measurable (if feasible); take into account the current requirements; must be monitored; be brought to the attention of authorised persons; if necessary, must be updated.

The Exchange Executive Bodies approve BCMS goals and the BC Manager keeps the documented goals.

9. Business Continuity Risk and Threat Assessment

The Business Continuity Risk and Threat Assessment (hereinafter referred to as the “Assessment”) is a part of the overall risk management system of the Exchange. The Assessment is carried out on a regular basis.

The Assessment has the following purposes:

- identification of threats, assessment and analysis of business continuity risks (emergency factors) in relation to the principle activities of the Exchange and the resources supporting them;
- Identification of threats which may lead to outages, errors and/or failure of software and hardware and software and hardware status monitoring tools, in particular, relating to their updates.
- determination of the need and a list of additional measures to reduce the risks of continuity.

The assessment is aimed at ensuring the manageability of business continuity risks and mitigating the consequences and probability of these risks occurrence, and significantly overlaps with the corporate operational risk management process in accordance with the Exchange's Operational Risk Management Policy.

While identifying business continuity threats, the most dangerous and/or probable threats from international practice and (or) reports of research organisations are taken into account as well as the Exchange-specific threats are determined.

Based on the results of threat identification, an internal document “Business Continuity Threat Map” is drafted. The document is approved by the Chairman of the Executive Board of the Exchange.

While assessing risks and threats to business continuity, it is necessary to determine the inherent risk level, the presence of controls, and/or, if necessary, measures that reduce the probability or impact of risk occurrence, the actual risk level in accordance with internal documents of the Exchange in the field of risk management.

The BC Manager continuously monitors business continuity risk events in the Exchange, investigates their reasons and circumstances and determines the required corrective actions.

The methodology and procedure for organising the Assessment, along with its frequency, are defined in a separate document “Business Continuity Risks Assessment. Process Description”.

10. Business Impact Analysis (BIA)

Business Impact Analysis (hereinafter referred to as the “Analysis”) is carried out to determine the processes with critical consequences if the Exchange’s processes are interrupted in case of emergencies or risk or occurrences or business continuity threat events depending on their duration.

The Analysis is carried out by all Exchange divisions in respect of their processes in accordance with the register of processes valid at the date of Analysis.

Based on the results of the Analysis, a report is prepared. The report shall determine the following:

- a list of critical processes and the impact of their downtime on the Exchange's business, including the possibility of providing critical services and the Exchange's services in a regular manner;
- a list of software and hardware, which failures and/or errors lead to disruption of these critical processes;

- internal and external resources, the availability and functioning (operability) of which are required to be in place and functioning to perform these critical processes;
- processes' recovery time target, including for critical processes;
- a list of critical service providers.

The scope and frequency of the Analysis are determined on the basis of changes in the internal and external conditions and processes of the Exchange and must have, at least, the following frequency:

annually for critical activities;

at least every two years for non-critical subdivisions (full cycle)

If required, it shall be allowed to carry out additional Analysis for individual processes in order to determine their criticality and recovery target value outside the frameworks of the general Analysis.

The Analysis methodology and procedure is determined by the internal document "Business Impact Analysis. Process Description".

Assessment and Analysis findings are used to develop (update) the Business Continuity Strategy for the next period.

11. Backup Infrastructure Facilities

To ensure that critical processes are resumed in the event of emergency, risk occurrence or threats to business continuity, the Exchange arranges for the operation of the backup software and hardware facilities.

For divisions implementing critical processes, workplaces are located at the backup site (mobile office/backup office/backup workplaces), which allow to carry out operations in the event of an emergency while the main office building used in the normal operation mode is unavailable.

Backup infrastructure facilities shall meet the following requirements:

- be located in a separate building(s) other than the main building(s);
- be geographically separate from primary infrastructure facilities at a distance ensuring the possibility for employees to resume critical processes of the Exchange within two hours from the emergency occurrence;
- ensure that it is possible to take measures to keep backup infrastructure facilities in such a condition ensuring resumption of the Exchange's critical processes within two hours, should they be not possible to implement at the main backup infrastructure facilities;
- ensure that electric power generators are available and maintainable;
- ensure that software and hardware of the backup complex can be maintained by at least two telecommunication service providers.

The Exchange BC Plan establishes the decision-making procedure for resuming the Exchange's critical processes in a backup software and hardware complex and/or relocating employees to a backup site.

12. Emergency Scenarios

Based on the results of the Business Continuity Risk and Threat Assessment, there shall be determined a list and description of emergency scenarios and related factors of business processes disruption in the normal operation, which will be responded within the BC framework.

Basic list of emergency scenarios:

- total/partial loss of the building;
- total/partial loss of Software and Hardware Complex;
- significant loss/unavailability of employees;

- problems on the suppliers' side/refusal of suppliers to provide goods/services.

In the course of BCMS operation, critical processes disturbances are manifested that were not previously taken into account (both new and not obvious) which may lead to new emergency scenarios.

Updating the basic list of scenarios (amending internal regulatory framework) can be done based on the result of response to a threat or in normal operation mode. Such updates are documented in the BC Plan.

13. Business Continuity Strategy

The Business Continuity Strategy is an internal BCMS document developed is developed in line with the strategic development directions based on business impact analysis and risks and continuity threat assessment findings. It describes the essential strategies chosen by the Exchange to ensure business continuity in the event of potential scenarios of critical processes disruption relevant for the Exchange. The supported business continuity strategies comprise one or more business continuity organisation and technology solutions under critical process disruption scenarios.

In defining the Strategy, the following factors shall be taken into account:

- maximum permissible duration of an emergency;
- the cost of implementing the Strategy and the consequences of omission.

The BCA Supervisor is responsible for the Strategy development. The authorised body of the Exchange approves the developed document. The Strategy shall be revised at least once in three years as well as in case of significant changes in the Exchange operation, the BC Policy, the organisational or technical infrastructure of the Exchange as well as in case of identification of new threats to business continuity that the current Strategy does not respond to.

14. Business Continuity & Recovery Plans

Business continuity and recovery plans shall be developed on the basis of the results of the Business Data Impact Analysis taking into account the approaches defined in the Strategy.

The basic set of business continuity assurance and disaster recovery documents comprise the following components:

- The Exchange BC Plan is a company-level plan that outlines overall cross-functional tasks of the Exchange, procedures, methods and timeframe to implement a set of measures to prevent or timely eliminate the consequences of a potential violation of the Exchange normal operation.

- The Divisional BCR plans are internal documents of the Exchange describing the actions to be taken by Exchange's divisions to timely recover their critical processes after the announcement of the emergency mode and before reversion to normal operation.

The current versions of the above-mentioned Plans shall be stored in places accessible to all employees involved in their implementation, in hard copy and in electronic form.

Besides, separate Plans could be developed for specific scenarios of loss of continuity, for example, a pandemic, restrictions on infrastructure or sanctions imposition. The need to develop or update such Plans shall be determined based on the current level of associated risks and the BC Supervisor's decision. These separate Plans shall be approved by the authorised management body of the Exchange.

The Exchange BC Plan

The Exchange BC Plan includes at least the following information:

- objectives, priorities and tasks to be resolved within the BC Plan;
- duties and responsibilities of BCMS participants;
- considered business continuity failure scenarios and associated disruption factors;

- general procedure for alerting and interaction of BCMS participants in response and elimination of emergency situations (taking into account the interchangeability of employees);
- procedure for internal reporting on emergency situations;
- procedure for the PERC to convene a meeting, make a decision on transition to the emergency mode and activating the BC Plan, BCR Plans and/or Software and Hardware Complex Recovery Plans;
- contact details of emergency operational services (phone numbers) and internal contacts (phone numbers, e-mail addresses) of individuals involved in implementation of measures to restore normal activities for the provision of significant services;
- basic requirements for the backup office;
- evacuation procedure and/or transfer to the backup office details;
- procedure for interaction between the employees and PERC/IERC;
- procedure for notifying stakeholders (clients, counterparties, the Bank of Russia, Moscow Exchange Group companies);
- procedure for termination of work in emergency mode and reverse to the normal operation mode.

The Exchange BC Plan shall be revised at least every year or more often in case of amendments to the Strategy, Policy, the Exchange's approach in terms of business continuity management, regulatory requirements, and in other cases requiring changing the general approach of the Exchange BC.

The BC Manager shall be responsible for the elaboration, review and update of the Exchange BC Plan. The BC Supervisor supervises and gets the Exchange BC Plan agreed upon.

The Exchange BC Plan shall be approved by the Exchange Supervisory Board in the predetermined procedure.

Divisional BCR Plans

BCR plans must be developed for Exchange's divisions (including those within a Centre of Excellence) having critical processes according to the business impact analysis. For those departments that do not have critical processes according to the business impact analysis, BCR Plans may be developed optionally by the decision of the Head of the Division with the use of a common template.

While developing BCR Plans, the most negative scenario shall be taken into account, that is complete loss of the main office, which implies the most negative consequence from each of the threats to business continuity. In case of less negative scenarios, separate blocks of the Plans shall be implemented. while developing BCR Plans. the need to ensure processes performance from the location of the backup office within 30 days should be taken into account.

The BCR plans of Divisions shall include detailed information on the response of the division's employees in the event of an emergency and at least the following information (or a reference to an additional BC document):

- a list of critical processes that a Division owns or participates in, with recovery targets and the resources required;
- the composition of Recovery Teams for a Division, their tasks (instructions for the Manager and Team members, containing a procedure to restore and maintain critical processes) and the required contact details;
- instructions for Divisions and employees with a description of actions required to maintain or timely restore normal operation for the provision of significant services;
- equipping the workplaces of the Teams in the backup office.

The Division Head is the owner and responsible for the development of the Divisional BCR Plan and the relevance of information it contains. It is the Division's BC Coordinator who is directly in charge of the development of the Divisional BCR Plan. The BC Manager provides methodological support and controls the resulting document.

The Division Head/ Head of the Centre of Excellence independently approves the Divisional BCR Plan in accordance with the established procedure.

The Divisional BCR plans are revised and updates annually. Updated are also made in the event of changes in the operating conditions of the Division that impact the efficiency of the current version of the Plan, and the results of BCMS tests conducted.

To decide on the need to update the current version of the division's BCR Plan, the Divisional BC Coordinators monitor, at least, the following events within their Division:

- new or changed/discontinued business processes;
- personnel changes, changes in contact information (taking into account the impact on the composition of the Recovery Team);
- change of the resources required for the performance of critical processes

Specifics of ensuring business continuity and operational reliability of the financial platform operator

The activity of the financial platform's operator is carried out by several divisions of the Exchange each of which has an their Divisional BCR Plan. At the same time, in accordance with the requirements for operational reliability while performing financial platform-based transactions, the financial platform operator must determine in internal documents the values of the target indicators of operational reliability:

- permissible downtime and (or) degradation of technological processes;
- total downtime and (or) degradation of technological processes during a calendar month;
- permissible ratio of the total number of financial transactions executed during the degradation of technological processes within the frameworks of an event or series of related events caused by information threats that have led or may have led to the disruption of the uninterrupted operation of software and hardware, should the permissible downtime and/or degradation of technological processes be exceeded, to the expected number of financial transactions for the same period in case of uninterrupted operation of software and hardware calculated on the basis of statistical data for the period of at least one year;
- indicator of compliance with the mode of operation (functioning) of the financial platform (start time, end time, duration and sequence of procedures performed on the financial platform to ensure the possibility of financial transactions execution).

These metrics can be included in other internal documents of the financial platform operator, other that BCR Plan.

15. Software and Hardware Complex Recovery Plan

The IT Unit shall provide backup and restoration of critical software and hardware tools and the required IT infrastructure and provide access thereto in case of emergencies.

Backing-up requirements for critical software and hardware tools shall be formed at the stage of the Business Impact Analysis by comparing the requirements of the owners of business processes/systems with the technical capability and cost of providing the required recovery target parameters. The requirements of the IT Infrastructure Technical Policy shall be taken into account as well.

The procedure for backup and recovery after the interruption of critical software and hardware tools shall be defined in the Software and Hardware Complex Recovery Plan which could be drawn up in electronic form. The Software and Hardware Complex Recovery Plan should contain at least the following:

- a list of critical software and hardware tools with the indication of the backup/disaster recovery solutions to be applied;
- members of critical software and hardware tools recovery teams, contact details;
- IT system recovery procedure, instructions/regulations for responsible employees.

The Software and Hardware Complex Recovery Plan shall be updated within the period specified therein and should amendments be introduced impacting its operability, or in case of noncompliance revealed by the results of testing.

The IT Unit shall be the owner and responsible Division for the Software and Hardware Complex Recovery Plan update. The BC Manager shall monitor compliance with these requirements.

16. BCMS Testing

BCMS tests are key components to keep BCMS up-to-date, and they are carried out regularly to determine:

- the level of readiness of the Exchange employees to promptly respond to emergencies, perform critical processes in the emergency mode and reverse to the normal operation mode;
- organisational and technical feasibility to restore critical processes within the required timeframe;
- sufficiency of RC equipment;
- coordinated interactions with Moscow Exchange Group companies under emergency conditions;
- adequacy of the level of BCMS regulation, completeness and correctness of information of the BC Plan, BCR Plans and Software and Hardware Complex Recovery Plans;
- measures required for further improvement and improvement of BCMS.

The BC Manager develops BCMS Test Program which should provide for rotation of various types of test activities and ensure adequate coverage of the BC Plan, BCR Plans, Software and Hardware Complex Recovery Plan and procedures for response, recovery and support of operations in case of emergencies. The BCMS Testing program is to be agreed with the BC Supervisor and by the authorised management body of the Exchange in its area of responsibility. The program can be adjusted based on the results of the activities performed and in case of significant changes in BCMS document support.

Tests should be carried out without prejudice to the principle activities of the Exchange and taking into account current economic, social, political and sanitary-epidemiological situation.

Full-scale BC Plan Testing, with the involvement of the Exchange employees engaged in the recovery of critical processes, shall be carried out at least once a year with regard to the external factors (regulatory restrictions, etc.). In the presence of these factors, the BC Supervisor may decide to postpone the full-scale testing with a justification for this.

Tests on fail-safe solutions for critical software and hardware tools deployed in a backup Software and Hardware Complex are done at least once a year and can be run on the same day as a full-scale test.

Each test shall include the following stages:

- planning and preparation of testing;
- conduct of testing
- execution, approval and distribution of a report on the test results with the mandatory analysis of the test results and development of measures to eliminate identified shortcomings;
- making a decision on whether BCMS documents should be revised or not.

A unified approach to the procedure for organising and conducting the necessary tests is ensured by the provisions of the internal document “Testing of Business Continuity Management System procedures. Process description” which determines:

- types, methods and frequency of testing;
- Divisions’ areas of responsibility when testing;
- recommended list of test participants;
- list and templates of mandatory documents generated within the frameworks of testing events (plans, protocols, checklists, reports);
- requirements for the provision and storage of test results.

17. Employees Training and Raising Awareness

To ensure that the Exchange is resilient to emergencies, and BCMS is efficient BCMS, as well as to achieve the required level of awareness of the Exchange employees and their understanding of their roles within BCMS, as well as employees' readiness to respond to emergencies, the Exchange offers training and awareness-raising events for its employees, including: The BC Manager develops proposals concerning employees' BC awareness and engagement, training materials and events to raise the BC culture.

To increase employee involvement in the BC system, the Exchange has ensured:

- familiarisation with this Policy and the BC Plan posted on the Exchange internal corporate portal;
- familiarisation with the BCR Plan of the Division;
- familiarisation with other BC documents, in particular, those concerning employee's actions in the event of emergencies.
- assigning internal e-courses on BC to employees;
- involvement of employees in BC tabletop exercises (testing);
- delivery of in-person consultations on BC issues (if necessary);
- information mailings concerning BC;
- maintaining the BC page of the Exchange corporate portal up-to-date.

18. BCMS while Interacting with Counterparties

Within the frameworks of BCMS, interaction with internal and external counterparties of the Exchange is considered to ensure uninterrupted service delivery or goods supply, including in the event of an emergency. For these purposes the Exchange Divisions determine the lists of strategically important (critical) counterparties of the Exchange Divisions (if any) and provide for alternative methods of implementing the processes in the event of critical counterparty scenario loss.

In case of interaction with a counterparty that is critical for the Exchange operations, it is recommended to provide for clauses in the contract regulating the interaction and responsibility of the parties in risks implementation and work in the emergency mode, taking into account the established deadlines and other required parameters of BCMS division. Additional analysis could be carried out for the counterparties of the divisions that are critical for the Exchange operation, in particular: Analysis of the Exchange counterparty's BCR Policy and/or BCR Plan (if any); exposure of the Exchange's counterparty to a group of risks with intent to minimise the risk groups similar the Exchange; readiness of the counterparty to work in emergency situations. The analysis could be carried out in electronic form once a contract with a counterparty is executed or the Division's BCR Plan is revised, if required.

19. Monitoring and Assessment of BCMS Efficiency

In accordance with BCMS lifecycle established by this Policy, monitoring and periodic assessment of the BCMS efficiency shall be carried out. The methodology for the procedure shall be envisaged in the document "Monitoring, Measurement, Analysis and Assessment of BCMS. Process Description". The results of BCMS monitoring shall be included in BCMS reports.

Monitoring and assessment of the BCMS is an integral tool for management which is used by the management and other stakeholders to achieve the required level of confidence that the Exchange will handle the risks and threats associated with business continuity.

The system of key performance indicators (KPI) for BCMS management is introduced to control BCMS state and operation, which indicates that:

- preventive measures of the Exchange are effective, performing properly and permit to achieve the goals set for BCMS (monitoring, analysis, testing);

- the Exchange management is informed about the preventive measures that are used in the company (reporting to the management);

- the implemented KPI system permits to characterise the maturity of BCMS processes and its scope.

BCSM monitoring and assessment results are integrated into the reporting system as part of the non-financial risk management process. All reports generated shall be kept as evidence of the results obtained.

20. BCMS Audit

BCMS shall be subject to audit. Internal Audit of BCMS is done at least once in three years by the Internal Audit team of the Exchange to continuously improve BCMS efficiency, to prevent BCMS inconsistencies, as well as to control the compliance of BCMS with:

- the regulatory documents of the Russian Federation, including regulatory documents of the Bank of Russia that regulate the issues of uninterrupted operation of the Russian financial market participants;

- requirements of internal documents, strategy and concepts of the Exchange.

The external ISO 22301:2019 compliance audit on BCSM is done by decision of the authorised management body of the Exchange.

Based on the results of an internal or external audit, nonconformities are identified, recommendations are made to eliminate them, or recommendations are issued to improve BCMS, the required corrective measures are developed which further contributes to the continuous improvement of BCMS performance and efficiency.

21. Control On the Part of The Exchange Management

Control on the part of the management is one of the most important components of the efficient BCMS operation.

Interim results of BCMS operation are discussed and analysed on an ongoing basis at scheduled and special meetings of Non-Financial Risk and Information Security Management Committee of the Exchange, as well as at operational meetings (if required).

The analysis of BCMS by the top management is carried out annually. Report on BCMS performance is submitted to the authorised Exchange management body for consideration and contributes to making informed tactical and strategic management decisions. All reports generated shall be kept as evidence of the results obtained.

The BC Manager shall ensure that the following materials be prepared for the management by the BC Supervisor within the BCMS reporting:

- the status of the implemented BCMS activities based on the results of the previous report;

- changes or proposals to change external and internal issues with regard to the Exchange BCMS;

- the results of the review of emergency factors upon the regular review of the business continuity threat map;

- consolidated reports on the failures and other occurrences of business continuity risks or threats triggering activation of the BC Plan;

- report on the results of the BC Plan testing performed;

- monitoring and assessment of the level of maturity of BCMS current capabilities and areas for improvement;

- identified nonconformities in BCMS and measures taken to correct BCMS;

- identified needs for changes to BCMS documentation, including this Policy and (or) BCMS goals;

- information on procedures and resources that may affect the improvement of BCMS efficiency;

- the results of Business Impact Analysis and Business Continuity Risk and Threat Assessment for the reporting period;

- the results of assessment of BCMS document support;

- risks and issues that need to be considered and discussed once again subsequent to the previous review;
- proposals and opportunities for continuous improvement and enhancement of BCMS.

Following the review of the submitted reports, a documented management analysis of BCMS shall be prepared encompassing the issues considered, the decisions taken, as well as the decisions related to the continuous improvement of BCMS capabilities and the identified needs for changes to BCMS in order to improve its efficiency and effectiveness. The results of the analysis shall be documented, stored by the BC Manager and could be provided to the stakeholders upon request.

22. Continuous Improvement of BCMS

The process of BCMS improvement is continuous and supported by the Exchange management control. The BC Supervisory controls the process. The process shall include, but not limited to:

- a regular assessment of the applicability and efficiency of implemented BCMS procedures, strategies, decisions, and plans;
- a regular assessment of BCMS document support relevance and making changes promptly;
- interactions with the operational risks division in order to identify new risks and to reduce the probability of occurrence or impact of existing risks;
- introduction of new BC technologies and automation of BC processes;
- promotion of BC corporate culture in day-to-day operations of the Exchange;
- up-skilling of BCMS employees supervising BC issues
- Reviewing findings of internal and external audits of BCMS and ensuring that identified non-conformities of the NHSMS are eliminated;
- adoption of best global practices and approaches in the field of business continuity assurance.

BCMS improvement full cycle shall be carried out at least once every three years or earlier when the BC Plan is activated; BC risk or threat occurrence, or in event of significant BC changes.

The results of the analyses carried out as part of the improvement process (both the full cycle of the analysis and the partially completed analysis) are included in the annual BCMS reporting.

23. Disclosure of BCMS Internal Documents

Except for this Policy, all the documents regulating BC developed by the Exchange shall not be disclosed. In the event of a request for information on BC, the Exchange submits a document describing general provisions regarding BC processes.

Other BC documents could be disclosed only in cases determined under the legislation of the Russian Federation.

24. Revision and Amendment of the BC Policy

This Policy is subject to periodic review at least once in three years.

The BC Policy shall be revised and/or amended in the following cases:

- amendments to the regulatory framework that affects BCMS;
- changing the Exchange's activities and/or adding a new type of activity within the BCSM scope;
- changing the Exchange's goals, concepts and strategy
- in case the test/analysis on BCSM and other procedures identify the need for changes in BCSM;
- when defining new efficient approaches to BCMS as part of BCMS continuous improvement

When revising/changing the Policy, it is required to:

- get agreed on the adopted changes, including in the procedures/approaches of BCMS, with the responsible persons involved in the BC and the management of the Exchange;
- make appropriate changes to the structure and text of the Policy;
- approve the Policy in the predetermined procedure;
- familiarise employees of Divisions with the Policy by sending it by e-mail and publishing it on the internal information portal for documents;
- make changes to the required BCMS elements