BULGARIAN STOCK EXCHANGE

RULES AND REGULATIONS

PART VI
RISK MANAGEMENT RULES

Chapter One
GENERAL PROVISIONS

Article 1. These Risk Management Rules are part of the Rules and Regulations of the Exchange and govern:
1. the identification of possible threats or risks that may cause potential losses or disruption of trading processes that are ensured, implemented and maintained by the Exchange;
2. the means of control and management of identified threats or risks;
3. the allocation of risk management responsibilities among Exchange employees.

Article 2. The risk management policy of the Exchange shall include:
1. the procedures for identifying risks related to the activities implemented by the Exchange and the systems operated by the Exchange and, where appropriate, for defining the acceptable level of risk;
2. procedures and measures to manage risks related to the activities, processes and systems of the Exchange;
3. mechanisms to monitor the adequacy and effectiveness of the policy and procedures referred to in item 1, and the level of compliance by the Exchange and by persons working under contracts for the Exchange with the procedures and measures referred to in item 2;
4. mechanisms to monitor the adequacy and effectiveness of measures taken to address any deficiencies or non-conformities in the policy and procedures referred to in item 1 and the procedures and measures referred to in item 2, including failures by the relevant persons to comply with such policy, procedures and measures.

Chapter Two
ALLOCATION OF RESPONSIBILITIES

Article 3. The following persons shall be engaged in risk management:
1. the Board of Directors;
2. the Chief Executive Officer;
3. the directors of directorates;
4. employees working under contracts at the Exchange.

Article 4. The Board of Directors shall have the following risk management responsibilities:
1. make decisions and issue orders regarding risk management;
2. review and assess, at least once a year, the results achieved in risk management.

Article 5. The Chief Executive Officer shall have the following risk management responsibilities:
1. monitor unacceptable risks, change of risks/levels of risk and risk management processes;

2. approve the risk mitigation measures proposed by the directors of directorates on the basis of the results of the assessment of the various types of risk;
3. approve taking specific steps to mitigate risks, introduce control mechanisms, and establish internal control standards;
4. approve decisions on personnel, logistical or methodological resourcing of risk management activities;
5. at least once quarterly, submit a report to the Board on the state of risk management systems;
6. make day-to-day decisions regarding risk management.

Article 6. The directors of directorates shall have the following risk management responsibilities:
1. organise work for proper implementation of the risk management policy as adopted by the Board of Directors;
2. control the policy and procedures applied by employees for identification of risks related to the activities of the Exchange and the mechanisms to monitor the adequacy and effectiveness of such policy and procedures;
3. inform the Chief Executive Officer of the number of detected incidents and the extent of damages caused, where such information is available;
4. approve and submit to the Chief Executive Officer for approval decisions on personnel, logistical and methodological resourcing of risk management activities;
5. implement the risk assessment process;
6. at least once quarterly, submit to the Chief Executive Officer a review and an assessment of the rules and, in case of any deficiencies, propose measures for improvement of risk management;
7. submit to the Chief Executive Officer for approval proposals for taking specific steps to mitigate risks, introduce control mechanisms, and establish internal control standards.

Article 7. The employees of the Exchange shall be required to get acquainted and comply with the procedures described in these Risk Management Rules.

Chapter Three
RISK MANAGEMENT POLICIES

Section One
GENERAL PROVISIONS

Article 8. (1) The risk management policy of the Exchange shall be implemented in an integrated manner and in line with all other policies and principles governed by internal regulations of the Exchange.

(2) The purpose of this policy is to document the measures and procedures for identification,

management, monitoring and assessment of risks related to the activities of the Exchange, in accordance with Article 86 (1), item 3 of the MFIA.

Section Two
TYPES OF RISKS AND MANAGEMENT PROCEDURES

Article 9. (1) The Exchange shall address the individual types of risks regarding its activities separately, unless the occurrence and management of such risks are closely related.

(2) The Exchange shall distinguish the following types of risks related to its activities, procedures and systems:
1. Internal risks: risks associated with the organisation of operation of the Exchange, being:
(a) process-related risks;
(b) system-related risks;
(c) personnel-related risk;
2. External risks: risks associated with macroeconomic, political or other factors that affect and/or may affect the activities of the Exchange, being:
(a) risks of environment;
(b) risks related to the physical and electronic security.

(3) Risk assessment shall be reported by the directors of directorates based on the results of the risk identification, assessment and control procedure described in Section Three.

(4) Based on the results reported according to the procedure, the Exchange shall define an acceptable level of risk for the organisation and shall ensure the performance of the activity within the limits of such defined acceptable level.

Article 10. (1) Process-related risks shall be as follows:
1. Risks associated with the performance of the principal functions of the Exchange:
(a) disruption of the continuity of trading in financial instruments;
(b) disruption of the continuity of operation of the Financial Instruments Trading System and the other information systems of the Exchange;
2. Risks associated with the services provided:
(a) culpably inflicted damage directly caused by the provision of false, inaccurate or incomplete data and/or analyses in connection with disclosure of information, public statements, etc.;
(b) use in bad faith of confidential information provided by members, issuers or clients (unauthorised access to confidential information) and breach of a trade secret;
(c) abuse of confidential information;
(d) conflict of interests;

(e) errors in the collection, entry or accounting of data;
(f) errors in supply of information to clients of the Exchange;
3. Project-related risks:
(a) budget risk associated with failure to comply with budget estimates;
(b) quality risk associated with the impossibility and/or inability to ensure project implementation within the pre-defined quality limits ensuring successful implementation of the project;
(c) risk of failure to meet deadlines, associated with the impossibility and/or inability to complete the project within the pre-defined and announced deadlines.
4. Risks associated with outsourcing operational functions in relation to the systems allowing or enabling algorithmic trading:
(a) the service provider is unable to perform the outsourced functions reliably and professionally and does not hold all required licenses or authorisations;
(b) the service provider fails to properly supervise the carrying out of the outsourced functions or to adequately manage risks associated with the outsourcing agreement;
(c) the outsourced services are not provided in accordance with the specifications of the outsourcing agreement, which are based on pre-determined methods for assessing the standard of performance of the service provider;
(d) the service provider fails to disclose to the Exchange any facts that may have a material impact on its ability to perform the outsourced functions effectively and in compliance with its legal obligations;
(e) the service provider fails to cooperate with the competent authorities with respect to the Exchange in connection with the outsourced activities;
(f) the service provider fails to comply with the requirements for protection of confidential information relating to the Exchange and its members, and to the Exchange's proprietary information and software.

(2) The procedures and measures for management of process-related risks shall include:
1. Regarding risks associated with the performance of the principal functions of the Exchange:
(a) drafting and/or conclusion of agreements on use of a financial instruments trading system;
(b) drafting and/or conclusion of agreements on use of an information system in connection with the trading carried out;
(c) maintenance and updating of the trading and information system;
(d) conclusion of an agreement with one or more depositary institutions or clearing houses in connection with the settlement of transactions in financial instruments;
2. Regarding risks associated with the services provided:
(a) development, adoption and implementation of a communication strategy of the Exchange;
(b) coordination of public statements of members of the Board of Directors and of Exchange employees with the Chief Executive Officer and, where necessary, with the Board as well;
(c) maintenance of systems and procedures ensuring the durable and confidential storage of

information on transactions concluded, as well as the information received from issuers in connection with their disclosure obligations;
(d) development and implementation of internal rules for handling information on the Exchange, introduction of privileges and access levels to Exchange information to ensure prevention of persons working for the Exchange under contract from disclosing and from using, for their own or other persons' benefit, any facts or circumstances concerning transactions concluded or financial results of issuers, and any other facts or circumstances constituting a trade secret, personal data and/or inside information that have come to their knowledge during the discharge of their official and professional duties;
(e) adoption and implementation of ethical rules of conduct of the Exchange staff members;
(f) ensuring full and up-to-date information on the Exchange's webpage regarding the services offered and the obligations of market participants;
3. Regarding project-related risks:
(a) unambiguous designation of the teams and allocation of responsibilities among employees in the development of a particular project;
(b) ensuring the use of persons offering competitive advantages or best conditions for implementation of the relevant project, where external consultants and/or subcontractors are used;
(c) development of terms of reference, a draft budget, and fixing deadlines for the implementation of each stage of the project;
(d) synchronising project-related public statements with the project manager;
(e) regular reporting of each stage of the project to the Chief Executive Officer, and current consulting in case of any problem or need to revise the original budget and/or terms of reference;
(f) acceptance of the completed project by the Chief Executive Officer or by the Board.
4. Regarding risks associated with outsourcing operational functions in relation to the systems allowing or enabling algorithmic trading:
(a) maintaining personnel having the necessary expertise to supervise the outsourced functions effectively and manage risks associated with the outsourcing agreement;
(b) taking swift actions if the service provider does not carry out the outsourced functions effectively and in compliance with applicable laws and regulatory requirements;
(c) enabling termination of the outsourcing agreement where necessary without detriment to the continuity and quality of services on the Exchange;
(d) ensuring effective access to data related to the outsourced activities;
(e) setting requirements to be met by the service providers to protect confidential information relating to the trading venue and its members, and to the venue's proprietary information and software;
(f) establishing, implementing and maintaining a contingency plan for disaster recovery and periodic testing of backup facilities, where that is necessary taking into account the operational function that has been outsourced.

Article 11. (1) System-related risks shall include:
1. full or partial unreliability and incomplete data;
2. subsequent occurrence of the problems with data reliability and completeness;
3. lack of precision in the processing methods;
4. software bugs;
5. imperfection of the technologies used;
6. failure in the system of the regulated market, the information and communication systems.

(2) The procedures and measures for management of systems risks shall include:
1. archiving the information system of the Exchange and maintenance of back-up systems;
2. procedure for recovery of the operability of the information system;
3. organisation and management of users' access to the information system, which precludes any inadvertent or intentional breaches of the integrity of the systems used by the Exchange;
4. defining various classes of information stored at the Exchange;
5. defining levels of access for the Exchange employees depending on their positions and the functions they perform;
6. regular auditing of the information systems;
7. establishing clear objectives and strategies in terms of business continuity;
8. allocating adequate human, technological and financial resources to pursue the objectives and strategies in terms of business continuity;
9. adoption and implementation of a business continuity plan, including any amendments thereof necessary as a consequence of organisational, technological and legal changes;
10. establishing a business continuity function within the Exchange.

(3) The Exchange shall develop and has an action plan available for emergency situations, which shall ensure the continuance and maintenance of normal operation for a sufficiently long period in compliance with the legal rules of operation.

Article 12. (1) Personnel risks shall be risks associated with losses due to:
1. resignation of key employees;
2. Exchange employees acting in bad faith;
3. insufficient qualification and lack of training of persons working for the Exchange under contract;
4. adverse revisions of the labour legislation;
5. unsecured safety of the working environment;
6. insufficient or inadequate motivation of employees;
7. frequent replacement of employees resulting in an impossibility to adequately perform the functions.

(2) The procedures and measures for management of personnel risks shall include:
1. clear definition of internal rules regarding the rights and duties of employees, and development of individual job descriptions that should be brought to the knowledge of the respective employees;
2. clearly defined levels of access to the information systems and databases of the Exchange;
3. regular personnel training on subjects related to financial theory and practice, risk management, the legal framework relevant to the activities of the Exchange, the information technologies and security, etc.;
4. regular meetings between the directors of directorates at the Exchange for sharing experience, perceptions and recommendations regarding the sources of risk and seeking solutions for risk management and minimisation;
5. discussions between directors of directorates and their employees, and personnel assessment once quarterly;
6. maintaining open communications among the various structural units of the Exchange;
7. initial and periodic safety at work briefing;
8. development and implementation of rules for health and safety at work;
9. development and implementation of internal wage rules in accordance with the job description of each of the employees;

Article 13. (1) Risks of environment shall include:
1. adverse revisions of the legal framework;
2. risks associated with the outsourcing of essential activities;
3. political changes;
4. amendments to the tax regulations.

(2) The procedures and measures for management of risks of environment shall include as a minimum:
1. maintenance of an up-to-date database of the legal framework relevant to the activities of the Exchange;
2. organising measures to monitor the compliance of implemented policies with the legal requirements and using external consultants and legal services in case of need to bring the activities of the Exchange into conformity with the legal requirements and any amendments thereto;
3. identifying clients, counterparties, etc. in accordance with the requirements of the Measures Against Money Laundering Act and the Measures Against the Financing of Terrorism Act, and the regulations on their implementation, in case of entering into a long-term relationship;
4. taking active part in public discussions regarding planned revisions of the legal framework concerning the activities of the Exchange and the capital market;

5. monitoring the effectiveness and the quality of performance of persons engaged by the Exchange in essential functions, based on existing agreements and, where necessary and possible, taking measures to remedy any deficiencies detected.

Article 14. (1) Risks of environment shall also include risks associated with physical and electronic security, such as:
1. natural disasters;
2. fire;
3. external fraud and theft;
4. acts of terrorism;
5. intrusion into the security systems;
6. unauthorised access to trading system or to a part thereof, including unauthorised access to the work space and data centres;
7. system interferences that seriously hinder or interrupt the functioning of the information system by inputting data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible;
8. data interferences that delete, damage, deteriorate, alter or suppress data on the information system, or render such data inaccessible;
9. interceptions by technical means of non-public transmissions of data to, from or within an information system, including electromagnetic emissions from an information system carrying such data.

(2) The procedures and measures for management of risks associated with physical and electronic security shall include:
1. ensuring an appropriate way for surveillance and control of the premises where the technological equipment and archives of the Exchange are located;
2. maintaining a constantly serviceable disaster centre ensuring continuity of the processes and, where this is impossible, prompt resumption of the processes;
3. regular preventive maintenance of the operational surveillance and control systems;
4. development of instructions on the access control system in the building of the Exchange;
5. development of a procedure for evacuation of employees in cases of immediate physical interference in the operation of the Exchange;
6. incident reporting procedure;
7. application of appropriate control mechanisms in connection with the electronic system, such as:
(a) a computer network firewall;
(b) network monitoring and analysis;
(c) data encryption;
(d) digital signatures;

(e) anti-virus software;
(f) backup copies of information;
(g) backup power supply;
(h) access control.

Section Three
RISK IDENTIFICATION, ASSESSMENT, MONITORING AND MITIGATION

Article 15. The risk identification, assessment and control procedure shall include the following phases:
1. risk identification, risk self-assessment and exercise of control;
2. assessment of the frequency of occurrence and the level of risk impact, and change in the level of risk, including the following activities:
(a) reporting risk measures;
(b) reporting incidents occurred.
3. risk monitoring, including monitoring of the change in risks and levels of risk and in the risk management processes;
4. risk mitigation, including the following activities:
(a) following-up the risk identified in audits;
(b) setting up control standards;
(c) insurance against risk.

Article 16. (1) Risk identification shall start with an internal investigation within the relevant unit, which shall be a fact-finding activity.

(2) In connection with risk identification, the directors of directorates shall inform the Chief Executive Officer in an appropriate manner of the number of incidents detected, including information on the extent of damage incurred.

Article 17. (1) The purpose of the process of risk self-assessment and exercise of control shall be:
1. to improve the timely identification of unidentified risks;
2. to improve the assessment of acceptability of the level of identified risks;
3. to further develop and improve alternative mechanisms for control of unacceptable risks;
4. to facilitate taking timely and accurate actions for risk mitigation;
5. to engage the individual structural units of the Exchange in the risk identification and assessment process, thus achieving greater responsibility of Exchange employees for risk management.

(2) The self-assessment and exercise of control results shall be used to determine the value of risk

measures for the individual business functions.

Article 18. (1) The value of risk measures provides information about the level of risk, whether the specific risks are within the pre-defined limits, and whether any actions need to be taken to mitigate such risks to a level acceptable for the company.

(2) The value of risk measures shall be determined on the basis of the risk self-assessment and exercise of control results.

(3) The directors of directorates shall identify the risk measures related to their activities.

(4) After the value of risk measures is assessed, the Chief Executive Officer shall determine realistic levels of risk tolerance.

(5) The directors of directorates shall immediately notify the Chief Executive Officer upon the occurrence or identification of new risk measures or values of risk measures exceeding the pre-defined limit values.

Article 19. (1) Actions taken in the risk assessment phase shall be predetermined by the results obtained in the risk identification phase. The assessment shall be determined by the relevant directorate which identifies the risk.

(2) Identified risks shall be analysed in terms of the following characteristics:
1. frequency of occurrence;
2. magnitude of impact.

(3) Based on this assessment, risks shall be categorised as acceptable or unacceptable, according to the level of risk defined as acceptable for the Exchange.

Article 20. (1) On the basis of the results of risk assessment, possible measures for risk mitigation shall be determined. Any residual risks after the implementation of the mitigation measures also need to be assessed.

(2) Risk mitigation shall be required where identified levels of risk exceed the levels defined as acceptable. Mitigation may be effected as follows:
1. avoidance of the relevant risk by discontinuing the activity which gives rise to the risk or by replacing such activity with an alternative activity;
2. reducing the probability of occurrence of the relevant risk by implementing control processes, improving the surveillance of activity, trainings;

3. mitigating the effect of manifestation of the relevant risk through insurance;
4. transfer of the relevant risk to third parties that are essentially exposed to the same type of risk;
5. prior identification and acceptance of a part of the effect of the relevant risk as intrinsic to the management bodies decision to proceed with the relevant activity.

(3) Risk mitigation measures shall be subject to approval by the Chief Executive Officer.

Article 21. (1) The risk monitoring process shall include taking specific actions for risk mitigation according to the measures approved. Taking such actions shall be the responsibility of the directors of directorates.

(2) Directors of directorates shall assist in implementing control mechanisms and setting internal control standards.

(3) Directors of directorates shall report to and coordinate their actions with the Chief Executive Officer.

Article 22. (1) The Exchange shall maintain an effective incident reporting mechanism the objective of which shall be:
1. to assist in forming a database of losses caused by operational incidents;
2. to help enhance the risk culture, and improvethe risk management process and the possibilities for risk mitigation accordingly by enhancing the information on the actual cost of operational risk;
3. to measure periodically the value of incidents occurring as a result of an operational risk, thus ensuring a better possibility for the management body to reduce costs;
4. to improve the possibility of responding to significant operational incidents;
5. to bring the requirements of the legal framework into conformity at the functional unit level;
6. to create a fully synchronised procedure for data collection and reporting, as well as avoidance of duplication of information and omissions.

(2) The risk management policy shall require immediate reporting of any incidents that are significant, of a threatening nature, having a bearing on the reputation of the company, or having an illegal or obscene effect.

ADDITIONAL PROVISIONS

§ 1. The terms used in these Rules, but not defined herein, shall have the meanings assigned to them in the POSA (Public Offering of Securities Act), the MFIA (Market in Financial Instruments Act), the IMAMAFIA (Implementation of Measures against Market Abuse of Financial Instruments Act) and their implementation regulations, or in the general commercial legislation or commercial

practice.

§ 2. For the purposes of these Rules:
1. 'Clearing' shall be the procedures for determination of the receivables and obligations of each of the Exchange members and the mutual offsetting of such receivables and obligations in connection with concluded transactions in financial instruments.
2. 'Settlement' shall be the procedures for fulfilment of the obligations to transfer cash and/or financial instruments in connection with transactions and their registration on an account with a depositary institution.
3. 'Depositary institution' shall be the Central Depository or another depositary of financial instruments, designated in compliance with the requirements of the MFIA.
4. 'Clearing house' shall be the Central Depository or another institution performing clearing functions, designated in compliance with the requirements of the MFIA.
5. 'Cross transaction' shall be a transaction in which the Exchange member who is the buyer and the Exchange member who is the seller are the same person.
6. 'Significant breach of official duties' shall be a breach defined as such in a statutory instrument or in internal regulations of the body that has defined the member as such, and that breaches the obligations of such member provided in such regulations. Assessment of the significance of a breach of regulations is made by the relevant competent authority and, in the case of internal regulations, the authority which defined the member as such.

§ 3. Terms and abbreviations used in these Rules:
1. 'The Exchange' means Bulgarian Stock Exchange AD, or the regulated market organised by Bulgarian Stock Exchange AD accordingly.
2. 'The Board' means the Board of Directors of Bulgarian Stock Exchange AD.
3. 'Chief Executive Officer' means the Chief Executive Officer of Bulgarian Stock Exchange AD.
4. 'FSC' means the Financial Supervision Commission.
5. 'CD' means Central Depository AD.
6. 'The System' means the electronic trading system through which Exchange trading is implemented.

TRANSITIONAL AND FINAL PROVISIONS

§ 1. These Rules shall take effect as of 23 February 2018.