DIRECTIVE ON THE INFORMATION, RISK MANAGEMENT, INTERNAL AUDIT AND INTERNAL CONTROL SYSTEMS OF TAKASBANK CENTRAL COUNTERPARTY MEMBERS

CONTENTS

FIRST SECTION **3**

The Objective, Scope, Grounds, Definitions and Abbreviations **3**

ARTICLE 1-The Objective 3

ARTICLE 2-The Scope 3

ARTICLE 3-The Grounds 3

ARTICLE 4-Definitions and abbreviations 3

SECOND SECTION **5**

General Principle **5**

ARTICLE 5- Establishment of internal audit, internal control and risk management systems 5

ARTICLE 6- Building information systems 5

ARTICLE 7- the responsibilities of Board of Directors 5

THIRD SECTION **5**

Risk Management System Principles **5**

ARTICLE 8- Risk management system 5

ARTICLE 9-Collateralization principles 6

ARTICLE 10- Stress tests 7

FOURTH SECTION **7**

Information System Management Principles **7**

ARTICLE 11-Information security 7

ARTICLE 12-Access and authorization 8

ARTICLE 13- ID verification 8

ARTICLE 14-Track records 8
ARTICLE 15-Primary systems 9
ARTICLE 16-Secondary systems 9
ARTICLE 17-Business sustainability 9
ARTICLE 18- Back-up 9
ARTICLE 19-Segregation of duties principle 10
ARTICLE 20- Physical security and environmental security 10
ARTICLE 21-Network security 10
FIFTH SECTION 11
Internal Audit Principles 11
ARTICLE 22-Internal audit system 11
ARTICLE 23-Periodic or risk based internal audit 11
ARTICLE 24-Internal audit plan 11
ARTICLE 25-Internal audit unit 12
ARTICLE 26-Internal audit operations 12
SIXTH SECTION 13
Internal Control Principles 13
ARTICLE 27-Internal Control System 13
ARTICLE 28-Internal control operations 13
SEVENTH SECTION 14
Various and Final Provisions 14
ARTICLE 29- Takasbank's authority to audit and request information 14
ARTICLE 30-Measures to take 14
ARTICLE 31-The situations that are not included in the directive 14
ARTICLE 32-Taking effect 14
ARTICLE 33- Implementation 14

DIRECTIVE ON INFORMATION, RISK MANAGEMENT, INTERNAL AUDIT AND INTERNAL CONTROL SYSTEMS OF TAKASBANK CENTRAL COUNTERPARTY MEMBERS

FIRST SECTION

The Objective, Scope, Grounds, Definitions and Abbreviations

ARTICLE 1-The Objective

(1) The objective of this directive is, to regulate the procedures and principles concerning the information systems, risk management, internal audit and internal control operations, that members who are deemed suitable to receive central counterparty service have to establish to manage the risks they assume due to their obligations to Takasbank, and to oversee the adequacy of these operations from the aspect of the Directive's provisions.

ARTICLE 2-The Scope

(1) The members that are authorized to trade at organized markets, where Takasbank serves as central counterparty and trading institutions, restricted to the obligations specified in the Istanbul Clearing, Settlement and Custody Bank Central Counterparty Regulation, Article 16, are covered by this Directive. The regulations concerning information systems, risk management, internal audit and internal control activities in the special legislation that the members are subjected to, are reserved.

ARTICLE 3-The Grounds

(1) This Directive has been prepared in reliance upon the Article 78, Paragraph 4 of Capital Markets Law, No 6362, which went into force following the release of Official Gazette No 28513, dated 30/12.2012, and Article 7, Paragraph 1, Subparagraph (ç) and Article 8, Paragraph 2 of Istanbul Clearing, Settlement and Custody Bank Inc. Central Counterparty Regulation, which went into force following the release of Official Gazette No 28735, dated 14/08.2013,.

ARTICLE 4-Definitions and abbreviations

(1) In the implementation of this Directive the following shall mean;

a) Direct Central Counterparty Membership: The members, who are authorized to perform clearing transactions only for themselves or their clients, pursuant to

provisions of Istanbul Clearing, Settlement and Custody Bank Inc. Central Counterparty Regulation,

b) General Central Counterparty Member: Pursuant to Istanbul Clearing, Settlement and Custody Bank Inc. Central Counterparty Regulation, members, who are authorized to perform clearing transactions of trading institutions besides themselves or their clients,

c) Trading Institution: Institutions who trade capital market instruments or at the markets where Takasbank provides CCP services, however are exempt from the obligations related to such transaction via a general CCP member,

d) **Track-record (Audit trail):** The records, which shall facilitate tracking a financial or operational transaction from beginning till end step by step,

e) Law: Capital Markets Law No 6362, Dated 06/12/2012

f) Board: Capital Markets Board,

g) CCP: Central Counterparty

h) CCP Service: Takasbank's activity, whereby it guarantees completion of clearing by assuming buyer role vs. seller and seller vs. buyer for an entire market or specific capital market instruments considered appropriate by the Board, via open bid, contract renewal or another legally binding method,

i) Central Counterparty Regulation: Istanbul Clearing, Settlement and Custody Bank Inc. Central Counterparty Regulation, which went into force following the release of Official Gazette no 28735 dated 14/08/2013,

j) Takasbank: Istanbul Clearing, Settlement and Custody Bank Inc.,

k) Member: General or direct central counterparty member, authorized to trade at the organized markets where Takasbank provides CCP services,

l) Executive Management: The member's general manager and assistant general managers and unit managers,

m) Board of Directors: The member's Board of Director

SECOND SECTION

General Principle

ARTICLE 5- Establishment of internal audit, internal control and risk management systems

(1) The members are obliged to build and operate adequate and effective internal audit, internal control and risk management systems, compatible with the range and structure of operations and capable of responding to changing conditions, to ensure follow-up and control of CCP services -provided by Takasbank- related risks that they are exposed to.

ARTICLE 6- Building information systems

(1) The Members are obliged to establish information systems that shall facilitate the security, sustainability and integrity of the data they produce, process, relay and keep, in relation to CCP services.

ARTICLE 7- The responsibilities of Board of Directors

(1) Establishing internal audit, internal control and risk management systems within the organization, operating such systems in an effective, adequate and proper manner, taking all kinds of measures towards the accuracy, soundness and maintenance of the data obtained from accounting and financial reporting system, and designation of authorities and responsibilities, lie with the board of directors.

THIRD SECTION

Risk Management System Principles

ARTICLE 8- Risk management system

(1) The objective of risk management system, is to ensure risk management through policies, implementation procedure and limits established at the minimum to follow-up, keep under control and if required mitigate the risks that the member is exposed to, due its operations at the markets, where Takasbank provides CCP service.

(2) The member calculates the risk that shall arise from existing and future positions at markets and capital markets instruments, that Takasbank provides CCP service, and collateral requirement, through methods compatible with Takasbank's methods.

(3) The member's risk management system is established and implemented to encompass the entire membership related activities, and the other processes, which could affect these activities.

(4) The risk management system, the fundamental principles and assumptions of the system and approval process for exceptional cases are put in writing in a clear and detailed manner, and take effect following board of directors' endorsement.

(5) The entire risk management system is reviewed at least once a year. The review process, in addition to compliance with CCP Regulation, at the minimum involves;

a) Verification of all the significant changes that occurred during risk measurement process,

b) Accuracy and completeness of position data,

c) Accuracy and completeness of collateral data,

d) Accuracy, completeness and compliance of position and credit limits,

e) Accuracy of collateral valuation methods.

(6) The member, pursues compliance to for CCP Regulation and the limits applied by Takasbank in the markets the member operates at, during the day and at the end of the day.

(7) The CCP member calculates and follows-up the changes that may occur in its guarantee fund contribution amount, as a result of risks that arise from its transactions and client positions.

(8) In the contract agreed between the general CCP member and the trading institution, authorization to independently execute risk reducing transaction on behalf of the trading institution is included, in case it is detected that the latter does not partially or fully serve its obligations and execution of risk reducing transaction is requested by the General CCP member, and the trading institution does not meet the request.

ARTICLE 9-Collateralization principles

(1) Collateral requirement calculation is at the minimum, based on the rules, methods and parameters determined by CCP.

(2) The member, before routing the orders to the Exchange's order systems, conducts the controls with respect to the measurement of risk that the portfolio or the client will be exposed to, following execution of the new order, and accordingly the additional collateral that shall be required if the order is accepted.

(3) The member builds limit control mechanism compliant with the position and risk limits specified in the procedures for the markets that Takasbank provides CCP service.

(4) The procedures concerning margining and collateral monitoring methods are written in a clear and detailed manner and take effect following the approval of the board of directors.

(5) The member informs its clients about margining method and use of collateral principles via the website. The clients are informed in writing, for only once at the outset, that such information shall be announced via the website.

(6) In regards to inputting margining parameters, at the minimum, control mechanisms are established, which shall prevent the alteration of the respective parameters by a single person and detect unauthorized alterations.

(7) Risk and collateral requirement calculations, are at the minimum, performed in parallel with the segregation enacted in the 25th Article of the CCP Regulation.

(8) The members, who trade at derivatives market, apply one of gross, net and/or portfolio based margining methods assigned by Takasbank for the respective market, and endorsed by the Board.

ARTICLE 10- Stress tests

(1) Stress tests are designed, in a way to encompass the factor and events that may significantly affect the members' financial situation, and by associating with the capital adequacy calculated pursuant to the provisions of "Communiqué Concerning Brokerage Firms' Capital and Capital Adequacy". The scenarios, which shall be employed in the stress tests, are prepared by taking into account the cases where significant losses occurred, albeit low probability, due to changes in factors such as underlying asset value, price volatility and interest rate, which could lead to extreme changes in risk provision or operational expenses or adversely affect risk management tools, and potential significant operational losses. Stress test result and the methodology and assumptions used in stress test are presented to the board of directors and it is ensured that these results are included into the decision-making mechanisms.

(2) Stress tests are conducted by general CCP members at least two times, for June and December terms, and by direct CCP members, at least once and for December term.

FOURTH SECTION

Information System Management Principles

ARTICLE 11-Information security

(1) Members classify hidden, relayed, processed and produced data from the aspect of confidentiality, accessibility and integrity, according to their degree of significance, to be sure that the information system security risks are managed at a satisfactory level,

and determine the minimum security controls required for these significance degrees, obtain Board of Directors' approval and operate the controls.

(2) General CCP members are obliged to ensure the confidentiality of the information pertaining to the trading institutions they serve as general CCP member, and the clients of these institutions, and access to this information should be restricted except the related personnel who have the necessity to know the information.

ARTICLE 12-Access and authorization

(1) In the operation of authorization process, the principle of assigning the lowest level of authorization by taking into account the job description, is the key consideration,

(2) Authorization mechanism is designed and operated, so as to prevent elevation of access rights of any user, party or systems by themselves without approval.

(3) The members keep track of the records at the widest possible level for privileged users and ensure that these records are reviewed regularly by people excluding these users and personnel associated with these users.

(4) Members establish authorization controls built according to confidentiality of accessible systems or data processes, and processes, and those controls shall be reviewed at least once a year.

ARTICLE 13- ID verification

(1) Members, establish ID verification controls built according to the confidentiality of accessible systems or data, and the processes, and those controls shall be reviewed at least once a year..

(2) The ID verifications that shall be applied are established to cover the entire period from the beginning of the session to the end.

(3) In remote access, controls, which shall guarantee the accuracy of ID verification data from the beginning of the session until the end, are established.

(4) ID verification data are stored encrypted and it is ensured that these data are encrypted with an up-to-date and secure encryption algorithm during the transfer of the data.

ARTICLE 14-Track records

(1) For authorization systems and the situations which may lead to changes in records at other critical systems, at the minimum, the track records including the information with respect to;

a) The person who accesses or attempts to access,

b) Transaction or attempt time,

c) The nature of the transaction or the attempt (create, update, delete, read or access)

are kept.

(2) Integrity and undeniability controls are established for the data stored with the member, and the executed processes, at a suitable level, and these controls are supported with sufficient track records.

(3) The track records held under the context of this article are stored for at least 5 years.

(4) Essential controls are established to disable the deletion or modification of the track records, by personnel, who have managerial rights at the systems that generate the records.

ARTICLE 15-Primary systems

(1) The member shall accommodates primary systems domestically, from where the IT services, supporting the functions that are critical in serving the membership obligations, are provided.

ARTICLE 16-Secondary systems

(1) The member shall accommodate the secondary systems domestically, which constitute the backup systems facilitating the fulfillment of the obligations in case primary systems are interrupted, from where IT services that support critical functions in serving the membership obligations.

ARTICLE 17-Business sustainability

(1) The member maintains sustainability of the IT services, which support critical functions in serving membership obligations. With this purpose, for IT services, it prepares business sustainability plans, where the rescue targets and tolerable disruption periods are determined, and sustainability actions coherent with these targets are laid out.

(2) The business sustainability plans, also contain rescue and return from backup processes, and it is ensured that the changes that occur in the respective services or systems, are reflected to the plans on a timely basis.

(3) The actions contained in the plans are regularly tested and the test results are reported to the executive management. The rest results are used in assessing if there is need to update sustainability plans, and if there is, the plan is updated by revisions.

ARTICLE 18- Back-up

(1) The data backup periods are determined in a compatible manner with the rescue targets in the business sustainability plan. At the minimum, the data, which is stipulated to be stored in the Directive, privileges, data processing infrastructure configurations, records and data base are backed up.

(2) It is ensured that the completed backups are stored in an area, where they shall not be under the same physical threats with primary systems and the same time. Appropriate storage conditions are provided to prevent the deterioration of backup cartridges, magnetic tape and similar environments, and to protect these environments.

(3) Controls are established to assure the completeness and integrity of the backed up data throughout the backup process and storage period

ARTICLE 19-Segregation of duties principle

(1) Segregation of duties principle is sought in information systems related implementation, development, testing, and system administration and operation functions. Under the framework of this principle, controls are established to prevent system entry, approval and completion of a critical transaction by a single personnel or single support service institution.

(2) In case it is not possible to fully serve the segregation of duties principle, risk responses, which shall mitigate risks against error and abuses that may arise from these situations or compensatory risk responses are applied. Such situations and the risk responses for these situations are endorsed by the Board of Directors.

ARTICLE 20-Physical security and environmental security

(1) Physical security measures are taken to protect information system infrastructure from fire, smoke, flood, earthquake and other natural disasters and power outage, explosion, burglary, terror and destruction events, at reasonable level.

(2) Physical security measures are taken to ensure that physical access to data processing infrastructure is only allowed for authorized persons.

ARTICLE 21-Network security

(1) Access is restricted to critical data processor elements both via the local network and the external network, and controls are established only allowing access to authorized uses and services.

(2) Communication security is provided for all remote access to data processing infrastructure. Controls are established to guarantee the accuracy of ID verification data from the beginning of the session until the end for remote access.

(3) Remotely accessible services are determined and accordingly, essential restrictions are arranged in the network infrastructure.

The essential measures are taken to identify and prevent potential attacks at the information system infrastructure.

FIFTH SECTION

Internal Audit Principles

ARTICLE 22-Internal audit system

(1) The objective of internal audit system, is to ensure assurance to executive management, that member activities are performed in alignment with the strategy, policy, principle and targets established by the Law and other respective legislation and the member, and on the effectiveness and adequacy of internal control and risk management systems.

(2) The members establish internal audit units to achieve the objective expected from internal audit system and keep enough number of staff at these units.

ARTICLE 23-Periodic or risk based internal audit

(1) Internal audit activities are performed based on risk assessments that also involve all sorts of risks that CCP activities engender.

(2) Risk assessments are conducted by the internal audit unit at least once a year, involving entire transactions, processes and services and seeking the following;

a) Transaction, process and services related regulatory issues,

b) The risks that transaction, process and services carry from membership aspect and the controls established against such risks,

c) In the case of existence of a designated risk management unit, the risk assessments conducted by such unit.

d) Significant regulatory changes notified by other units to the audit unit,

and presented to the Board of Directors.

(3) Executive management's opinions are taken for risk based audits, however the ultimate assessment decision, lies with the internal audit unit.

(4) Responsibilities involving regular review of risk-based audits, establishment of communication channels, which shall facilitate the reflection of changes that could affect the assessments, to the assessment, and update of assessments whenever required, lie with the audit unit.

(5) Membership legislation compliance is at least once a year, included into the internal audit activities.

ARTICLE 24-Internal audit plan

(1) Internal audit activity plans are based on conducted risk assessment.

(2) During the preparation of the plan, it is essential to include the significant planned changes in the structure of product and service, in the audit periods.

(3) In the internal audit plans, at the least;

a) Importance and risk rankings determined as a result of risk assessments,

b) The objective and targets of audit studies,

c) Summary risk assessments of the transaction, process and services that shall be audited,

d) The governing legislation for the audited transaction, process and services,

e) The planned time for the audit studies and audit period,

f) The resources required for the planned audit studies and the potential effect of resource constraints,

are included.

(4) Internal audit plan, takes effect following Board of Directors' approval.

ARTICLE 25-Internal audit unit

(1) An internal audit unit, directly reporting to board of directors, is designated to perform the internal audit activities. Internal audit unit, may also be designated under the supervision of non-executive audit committee established within the board of directors to assist in on site audit ad oversight activates.

(2) It is ensured that internal audit unit and audit personnel are not held accountable to answer to anyone aside from board of directors or audit committee.

(3) It is ensured that internal audit personnel, is provided access to the member's entire information and documents without any restriction, to serve their tasks.

ARTICLE 26-Internal audit operations

(1) The concluded internal audit studies are submitted to board of directors as a report. The audit studies, which constitute the basis for audit report, are documented in working papers, and such papers are delivered to audit unit with the end of audit studies, and kept for at least 5 years.

(2) In the internal audit reports, at least;

a) Audit scope and objectives,

b) Outcome of audit studies,

c) Identified problems,

d) Other information that may be required by the executive management

Are included.

(3) The activities of trading institutions, which are guaranteed by general CCP members, may be audited by the general CCP member's internal audit unit, under the condition that the principles are determined in the contract.

SIXTH SECTION

Internal Control Principles

ARTICLE 27-Internal Control System

(1) The objective of internal control system, is to ensure, protection of member and client assets, that the entire business and transactions, including non-central organization, are performed in coherence to the management strategies and policies, in a regular, efficient and effective manner, subject to the existing regulation and rules, the integrity and soundness of account and record order, availability of the information in the data system in a timely and accurate manner, prevention and detection of fault, fraud and irregularities.

(2) To be able to achieve the expected objective from the internal control system;

a) Establishing functional segregation of duties based on segregation of duties principle within the member, and distribution of responsibilities

b) Building accounting and financial reporting system, information system and communication channels,

c) Preparing business sustainability plan and other respective plans,

d) Establishing internal control activities,

e) Creating the work flow diagrams, that exhibit the member's controls over the business processes, and business steps, clearly identifying the points that shall be controlled on daily, weekly or monthly basis in such work flow procedures,

f) Entire internal control system policies and procedures which are put into writing and approved by the board of directors for implementation

are compulsory.

ARTICLE 28-Internal control operations

(1) The internal audit system activities are performed by board of directors, every rank of member's personnel and individually established internal audit unit; and in the absence of internal control unit, by the staff in charge of internal audit.

(2) The members' internal control activities are regulated and sustained so as to allow the follow-up of observed risks, and as an integral part of the daily activities.

(3) General CCP member, builds and operates an accounting system, that shall facilitate the segregation of the asset and liabilities of the trading institutions it serves as general CCP member and these institutions' clients, from the assets and liabilities of itself and its clients.

SEVENTH SECTION

Various and Final Provisions

ARTICLE 29- Takasbank's authority to audit and request information

(1) Takasbank, can request information from members at the frequency and in format which is customized according to the risk carried by the member, and it can conduct on-site audit at the members' headquarters and branches.

ARTICLE 30-Measures to take

(1) When it is detected by Takasbank, that the member's internal audit, internal control, risk management and information systems fall short of controlling and managing the risks related to CCP services that the member is a party to, as well as taking measures against the member, that are specified in the CCP Regulation and other respective legislation depending on the nature of the deficiencies, a reasonable deadline may also be assigned to remedy the deficiencies. Members, who cannot remedy their deficiencies by the deadline therefore are considered to have lost their membership eligibility, are subjected to 15th Article of the CCP Regulation.

ARTICLE 31-The situations that are not included in the directive

(1) The regulatory provisions that the member is governed by apply for situations that are not included in this Directive.

ARTICLE 32-Taking effect

(1) This Directive takes effect one year following the release date.

ARTICLE 33- Implementation

(1) The provisions of this Directive are implemented by the Takasbank Board of Directors.