DISCLAMER:
This is an informative translation, by no means BRSA can be held responsible for misstatements and misinterpretations here within.

REGULATION

From the Banking Regulation and Supervision Agency:

REGULATION ON INFORMATION SYSTEMS AUDIT TO BE MADE IN BANKS BY INDEPENDENT AUDIT INSTITUTIONS

SECTION ONE
General Provisions

Purpose

ARTICLE 1 – (1) The purpose of this Regulation is to lay down the principles and procedures concerning the audit of banks' information systems together with systems and process thereof related to production of financial data, by authorized independent audit institutions.

Scope

ARTICLE 2 – (1) Banks and partnerships thereof under the scope of consolidation to be limited with the aim of preparing information system audit report, outsource institutions providing information systems service to banks, institutions authorized to perform audit of information systems, independent audit institutions and companies providing fieldwork shall be subject to the provisions of this Regulation to be limited with the aim given in Article 1.

Legal Basis

ARTICLE 3 – (1) This Regulation is based on the provisions of Article 15 and Article 93(4) of the Banking Law dated October 19, 2005 Nr. 5411.

Definitions and abbreviations

ARTICLE 4 – (1) For the implementation of this Regulation, the following terms shall have the meanings indicated below;

a) Independent audit: the definition given in Article 5(1) of RPIA,

b) Independent audit institution: the institution granted the authority to make audit in banks pursuant to article 7 of RAIIA,

c) Bank: The bank defined in Article 3 of the Law,

d) RPIA: The Regulation on the Principles of Independent Audit published in the repeated Official Gazette dated 31/1/2002 Nr. 24657,

e) RAIIA: The Regulation on authorization of Institutions to perform Independent Audit and Temporary or Permanent Annulment of Authority Thereof published in the repeated Official Gazette dated 31/1/2002 Nr. 24657,

f) Information Systems Audit: The process whose principles and procedures are determined by a contract and which is comprised of the evaluation of quality, operations, adequacy, integrity, security, reliability and reporting of internal controls relating to whole information systems elements such as software and hardware used by the audited institution during their activities, information systems processes, information systems and processes used in financial data generating,

g) Auditor: Authorized profession personnel assigned by related institution authorized to make audit of information systems,

h) Audited institution: Banks as well as their partnerships under the scope of consolidation to be limited with the aim of preparing information system audit report,

i) Law: The Banking Law Nr. 5411,

j) Board: The Banking Regulation and Supervision Board,

k) Agency: The Banking Regulation and Supervision Agency,

l) Authorized institution: Independent audit institution being granted the authority to make audit on information systems,

m) Officer: Chairman and members of the audited institution's board of directors, committee of auditors and credit committee as well as general manager, assistant general managers thereof and the personnel binding the audited institution by their signatures.

SECTION TWO
Authorization and Staff

Qualifications Required for Institutions to be Authorized and Partners Thereof

ARTICLE 5 – (1) Institutions to make information system audit in banks are required;

a) to have the authority to make independent audit in banks,

b) to employ sufficient number of and auditors qualified enough to carry out the activities under the scope of this Regulation.

(2) In addition to the terms included in RPIA and RAIIA; it is obligatory that, partners of the authorized institution shall not take place as partners in the audited institution or in independent audit institutions whose authorization to make audit in companies subject to Capital Market Law Nr. 2499, or as independent auditors or auditors in an audit activity leading to annulment of authorization.

Information and documents required in application for authorization

ARTICLE 6 – (1) The following documents shall be attached to the application letter to be submitted to the Agency by the independent audit institution requesting to make information systems audit;

a) Auditors' noterially certified copies of , if there is any, Certificate of Information Systems Audit (CISA), documents relating to trainings received or given on issues under the scope of this Regulation,

b) Auditors' detailed curriculum vitae including their Professional experiences,

c) Judicial records of the auditors,

d) Auditors' statements declaring that they do not have partnerships in more than one independent audit institution and they do not take place as partners in the audited institution or in independent audit institutions whose authorization to make audit in companies subject to Capital Market Law Nr. 2499, or as independent auditors or auditors in an audit activity leading to annulment of authorization,

e) Auditors' statements declaring that they do not work in jobs other than their professional activities.

Granting the authorization to make information system audit

ARTICLE 7 – (1) As a result of the due-diligence made by the Agency for determining the professional and technical adequacies of the partners and auditors of the independent audit institutions which have made application for authorization to conduct information systems audit, within the scope of information and documents determined in the Article 6 of this Regulation, the above-mentioned authorized institutions are granted the authority to make information systems audit in banks upon Board resolution, on condition that there exist a conviction that they have an adequacy to execute the activity respects.

(2) The issues taken into consideration during the process of granting authorization to independent audit institutions can be reviewed by the Agency.

(3) Continuity of factors which enable to obtain the authorization to make information systems audit is essential. The Agency shall control the existence of such factors when it deems necessary.

(4) Titles of independent audit institutions which are granted the authority to make information systems audit shall be announced in the Agency's web site.

Annulment of the authority to make information systems audit

ARTICLE 8 – (1) In cases of the determination of one or more of the situations stated below, upon the evaluation made by the Agency, the board shall decide to annul temporarily or permanently the authorization to perform information systems audit of the authorized institutions which are determined to violate the provisions of this Regulation according to their violation nature.

a) arranging reports which do not reflect the real situation of the audited institution, or insufficient coverage, wrong or misleading documents relating to information systems,

b) in information systems audit performed, not carrying out or carrying out insufficiently the issues included in information systems audit contract,

c) replacement of the auditors without informing in advance the audited institution and the Agency,

d) not having performed information systems audit in audited institutions as of five accounting periods consequently,

e) not performing information systems audit in compliance with the provisions of this Regulation,

f) not obeying the notifications made by the Agency or repeating the issues subject to the notification,

g) if authorized institution and partners do not meet anymore the conditions determined in article 5 of this Regulation,

h) if the documents to be submitted pursuant to article 6 of this Regulation are fictitious,

i) not fulfilling the responsibilities determined in article 11 of this Regulation,

j) determining false transactions on the issues determined in other articles of this Regulation and under the responsibility of the authorized institution and the auditor,

k) if the audit plan and working papers are unable to proof the studies and findings on information systems audit made,

l) not having sufficient audit evidence,

m) not being unable to prove that the principles ad procedures defined in this Regulation are completely obeyed by the authorized institution, in case issues which can affect significantly the reliability of information systems and financial data generating process are determined,

n) not submitting the information and documents requested by the Agency.

(2) Before the permanent or temporary annulment of the authorization, the defense of the responsible person or institution is taken. In case of not granting the defense in one month as of the date of the communiqué related to the demand of defense, it is considered that the right of defense is waived.

(3) Within the time given by the Agency, to correct the non compliance to the regulations or to fulfill the responsibility of notification, the authorization of the institution authorized to make information systems audit could be temporarily annulled by the Agency.

(4) Within the scope of this Article, the fact that the authorization of the institution authorized to make information systems audit is annulled temporarily does not mean that its authorization to make independent audit is annulled as well. The fact that the authorized institution loses its authorization of independent audit requires the annulment of its license to audit the information systems.

(5) If the authorized institution realized the information systems audit by outsourcing within the framework of the Article 27 of this Regulation, the provisions of this Article are effective.

(6) The denominations of the institutions of which the authorization of information systems audit are annulled by the Agency are announced in the official web site of the Agency.

Employees’ Business Titles

ARTICLE 9 – (1) The auditors take the titles of chief auditor responsible for information systems, Chief auditor of information systems, senior auditor of information systems, auditor of information systems and assistant auditor of information systems, by seniority.

(2) The Chief Auditor responsible from information systems means the person having the title of Chief Auditor responsible for information systems, who conducts the audit of information systems on behalf of the authorized institution with his responsibility, and who has the authority to sign the information systems reports.

(3) Minimum 10 years of experience in information systems audit, Professional information systems control or safety is needed to gain the title of Chief Auditor responsible for information systems, 6 years is needed to become a senior information systems auditor, and 3 years is needed to become an information systems auditor. The experiences of auditors having the Certificate of Information Systems Auditor (CISA) and performed audits in the field of finance can be evaluated within this scope. The experience needed for Professional title is composed of time passed in one or all the subjects like information systems audit, Professional information systems control or security. The Certificate of Information Systems Auditor (CISA) is counted as one year of information systems audit experience, in addition to periods listed above. The persons whom knowledge, abilities and competences are not sufficient to pass to a higher seniority are not promoted to a higher seniority even if they fulfill their term.

(4) All of the employees charged with information systems audit in the institutions within the scope of this Regulation, shall certificate that they had or give education, for at least twenty-three hours a year and for at least one hundred and twenty hours in three years, within the scope of permanent education programs. The mentioned documents are maintained by the authorized institutions.

SECTION THREE
Liabilities of the Parties

Liabilities of under audit

ARTICLE 10 – (1) The party under audit is liable for information systems, relevant documentation, documentation concerning the financial information formation processes and any record, information, document, structure and application, the establishment, adequacy, productivity and effectiveness of every general and application controls within the scope of information systems and internal control system, and operate productively and effectively.

(2) The party under audit, before all else, must provide the information system document documentation, documentation concerning the financial information formation processes and any record, information, document, structure and systems for information systems auditing.

(3) The party under audit is liable for submitting any information and documents the auditor demands for information systems auditing.

(4) The party under audit is liable for notifying to the auditors all systems and applications they use in their activities and the application list which includes the usage aims. Application controls are determined, evaluated and reported by the party under audit for every system and application, which composes, supports, uses and saves financial data production processes and the data they include. In the evaluation of these controls, consistency of the systems to the written documentations, adequacy and application of written controls, safety, integrity and permanency of the data they include are reviewed.

(5) The party under audit establishes an environment concerning each process subject of general controls that take place in the Articles 14, 15, 16 and 17 of this Regulation, appropriate for the subjects, which are as follows:

a) Process owner: A process owner, whose liability is defined explicitly, is assigned for every process subject to general control.

b) Repeatability: Processes subject to general control are defined as being repeatable.

c) Targets and aims: Targets and aims defined explicitly are set for every process subject to general control in order that they operate effectively.

d) Roles and liabilities: Roles, activities and liabilities defined explicitly are set for every process subject to general control in order that they operate effectively.

e) Process performance: Performance of every general control process is measured according to the targets determined.

f) Policies, plans and procedures: Policies, plans and procedures concerning each general control process are written, reviewed periodically, updated, approved and announced to all interested units.

Liabilities of competent bodies and auditors

ARTICLE 11 – (1) The auditor is liable for giving information to the managers under audit all along the line about the errors and abuses arisen.

(2) It is obligatory that the changes in the information and declarations specified in the Article 6 of this Regulation be notified to the Agency in five workdays. Changes occurred in primary contract, administration and organization structures, and in the information systems audit staff are required to be notified on its grounds.

(3) Authorized institutions are liable for ensuring the information systems auditors they employ are attending the training programs continuously.

(4) Authorized institution is liable for notifying on its grounds and in five workdays to the Agency in such cases; when it resigns from the information systems during the contractual period or the contract is abolished.

(5) Information systems auditor is liable for; abiding the professional principles the profession necessitates and the audit principles determined in the ISAR, pursuant to this Regulation; preparing an information systems audit plan by considering the risks and weaknesses that might exist in information systems and within the scope of professional skepticism; submitting thereof to the party under

audit and practicing, taking exception to an audit evidence of the explanations of the managers and preparing the information systems audit report relating information systems and financial data formation processes.

(6) In case of improper applications, abuse or errors are confirmed during the information systems audit, even if the party under audit made up for the defects, it is obligatory that this subject is notified urgently to the Agency and managers by the information systems auditor and that the information system report is prepared within this scope, thereof. It is provisional that states, which require transition to the judicial sentence and which consist of crime are to be notified urgently to the Agency in writing.

(7) The auditor instantly informs the managers written or oral about every subject he considers significant, including the subjects occur during information systems auditing and which are indicated below, which are as follows:

a) General approach and scope of information system auditing, including the possible limitations and additional studies,

b) Disorganizations concerning the information systems policy formation process which have or may have an important influence on information systems, problems or changes in policy applications,

c) Ambiguities, which may raise doubts about the continuity of activities of banks,

d) Disagreements experienced with managers on subjects that may influence the information systems or information systems auditing report,

e) Fundamental weaknesses and risks take place in information systems.

(8) The auditor documents the evidence concerning about the matters notified in working sheets and the answers received in such cases when informing is done orally.

(9) The auditors are liable for saving the documentation and documents entrusted by the persons concerned within the scope of information systems auditing, in a period, which their work requires, and with honesty of purpose and without changing them. Competent bodies may keep copies of the documents, which forms audit evidence.

(10) Competent bodies and auditors shall not divulge the information, which they obtained on account of the information systems auditing activities and which is within the context of confidential information according to the provisions of the relevant regulation to anyone except the ones entitled explicitly by law and shall not use directly or indirectly for their own benefits.

(11) In the event of the information and documents concerning the information systems auditing are not submitted by the party under audit to the authorized institution this situation is notified urgently to the Agency.

(12) The auditor who obstructs the activity of information systems auditing systematically and effectively cannot serve in the information systems auditing of banks and his name cannot take place in the auditor list organized for this purpose.

(13) The authorized institutions are must to be conducting the independent financial audit independent audit activities of the party under audit in the period in which the information systems auditing is to be realized.

SECTION FOUR
Auditing Information Systems
Auditing the extent of information systems

ARTICLE 12 – (1) Considering the extent and structure of the activities of the party under audit, the authorized institutions are obliged to audit and evaluate general controls concerning the processes under the main titles of planning and organization, acquisition and implementation, services and support, monitoring and evaluation and application controls on information systems, within the scope of materiality principle; determine the situations according to the maturity model, which displays the level of information systems governance processes and report .

(2) The authorized institutions perform the information systems auditing and in care of auditors and assistant auditor. In order that the information systems auditing is performed, the independent auditing firm has the authority of information systems auditing and has made an information systems auditing contract with the party under audit, within the scope of this Regulation.

(3) Application controls are performed in accordance with the cooperation need between the auditors by the authorized professional employee who is defined as the auditor within the scope of RAIIA and the information systems auditor.

Auditing the types of information systems

ARTICLE 13 – (1) The information system auditing divided into three in extent. Which are; application controls auditing and auditing of general control areas; wide-ranging audit in which application controls and general control areas are performed together.

(2) Application controls are audited at least according to the controls disclosed in the Article 18 of this Regulation, in standards of applicability and to be of materiality criteria. Auditing of general control areas are performed by auditing the general control areas represented in the Articles 14, 15, 16 and 17 of this Regulation. The concept of application controls in this Regulation is used in parallel meaning to the internal audit system disclosed in the Regulation on Internal Audit of Banks and Risk Management Systems published in the Official Gazette dated February 8, 2001 and Nr. 24312.

(3) Application controls are audited every year, and general control areas are audited annually. The Board, if seen necessary, may differentiate the extent of any audit types and/or the audit frequency for any bank or all banks.

(4) The auditor evaluates the situation in which the party under audit shall establish pursuant to the Article 10 of this Regulation, during the auditing process.

Auditing the planning and organization activities

ARTICLE 14 – (1) In order to fulfill the occupational goals, planning and organization activities contains strategies and methods concerning the determination of giving information technologies support in the most appropriate way. Strategies that are planned so as to include different point of views are transmitted to the units and persons concerned within the organization. The fact that the technologic infrastructure operates profitably and effectively in a healthy organizational structure is taken into consideration within the process of information systems auditing.

(2) Within the scope of general controls concerning planning and organization, control objectives are audited concerning the processes of:

a) Defining strategic information technologies plan,

b) Defining the information architecture,

c) Defining technologic course,

d) Defining processes, organization and relations of information systems,

e) Information system investments management,

f) Transmitting targets and instructions of the management,

g) Human resources management,

h) Quality management,

i) Evaluation and management of information systems risk,

j) Project management.

Auditing the provision and execution activities

ARTICLE 15 – (1) Acquiring and implementing activities include defining the information technology solutions developing or obtaining from exterior supporters, practicing and unifying with work processes to realize information technology strategies. Maintenances and changes in the systems are also evaluated within this control area.

(2) Within the scope of general controls concerning acquisition and implementation, control objectives are audited concerning the processes of:

a) Determining automation solutions,

b) Developing and maintaining application software,

c) Constituting and maintaining technology infrastructure,

d) Providing operation and usage,

e) Providing the information systems resources,

f) Change management,

g) System analysis and changes being applied and accredited.

Auditing the services and support activities

ARTICLE 16 – (1) Service offered and support activities refer to offering the needed services safely and continuously including the required training.

(2) Within the scope of general controls concerning the services offered and support activities, control targets are audited concerning the processes of:

a) Defining and management of service levels,

b) Management of services received from third parties,

c) Performance and capacity management,

d) Providing service permanency,

e) Providing system security,

f) Determining and distributing costs,

g) Training of the users,

h) Management of service offered and event management,

i) Configuration management,

j) Problem management,

k) Data management,

l) Physical environment management,

m) Operation management.

Auditing the monitoring and evaluation activities

ARTICLE 17 – (1) Monitoring activities includes the periodical evaluation of the appropriateness and quality of the controls established concerning information technologies, by the party under audit.

(2) Within the scope of general controls concerning monitoring and evaluating, control objectives are audited concerning the processes of:

a) Monitoring and evaluating the information systems performance,

b) Monitoring and evaluating the internal control,

c) Providing the consistency of the party under audit to the relevant legislation including internal procedures and principles,

d) Ensuring corporate governance concerning information systems.

Application Controls of Information Systems

ARTICLE 18 – (1) Application controls include the audit and evaluation of adequacy and effectiveness of internal controls to be used in all work processes such as authorization of data access and determination, production, usage, integrity and reliability of financial data used for supporting and implementing banking activities in information systems.

(2) Application controls are the specialized controls, which take place in the controls of work cycle defining the controls on work processes and which are realized by computer aided and/or manual routines.

(3) Application Controls minimally includes the items below;

a) Data formation/authorization controls:

1) Data preparation procedures: The input form designs help to minimize the errors and deficiencies. The procedures of error handling used in the process of data formation ensure the determination, reporting and correction of the errors and disorders.

2) Source document authorization procedures: The authorized personnel prepare the source documents according to their appropriate privileges appropriately. Formation and approval of source documents is subject to segregation of duties principle.

3) Gathering the source document data: There shall exist procedures providing the integrity and correctness, accountability and timely submission of the authorized source documents.

4) Error handling in source documents: The procedures of error handling used in the process of data formation provide the determination, reporting and correction of the errors and irregularities.

5) The protection of source documents: There shall exist procedures providing the protection of the original documents for a definite period or the protection of them in reproducible way in order to reach the data whenever it is required.

b) Input controls:

1) Input authorization procedures: There shall exist procedures providing data input only from authorized sources.

2) Correctness, integrity and authorization controls: Transaction data produced by the personnel/the system, or entered via interfaces to be processed consequently are subject to various tests for correctness, integrity and validity controls. Besides, there shall be procedures providing the approval and alteration of the input data in the closest place to the source point.

3) Error handling in data inputs: There shall exist procedures providing the reprocessing and correcting of the data entered incorrect.

c) Data processing controls:

1) Integrity in data processing: Data processing procedures provide the compliance to the segregation of duties principle and validation of the works done. Those procedures also provide the existence of adequate updating controls such as run to run totals and master file updating controls.

2) Validation and change in data processing: There shall exist procedures providing approval, user validation and change realized close to the source.

3) Error handling in data processing: The procedures on error handling in data processing provide the determination of the errors before processing and prevents the interruption of other valid transactions.

d) Output controls:

1) Output handling and protection: Specified procedures shall be followed while handling and protecting the outputs of the application of information systems, confidentiality and security needs shall be taken into consideration.

2) Distribution of outputs: The procedures on distribution of the information systems outputs shall be defined, announced and followed.

3) Output checks and agreement: The confirmation of the outputs with the control totals shall be controlled routinely. Log records facilitate the pursuit of the transactions of operations and reaching an agreement on the problematic data.

4) Reviewing the outputs and handling the errors: There shall exist procedures enabling the appropriate users and persons providing the outputs to review the outputs and the correctness of the outputs. Besides, there shall be procedures on handling and defining the errors in outputs.

5) Ensuring the security of output reports: There shall exist procedures on the provision of the securities of output reports distributed to the users or waiting for distribution.

e) Boundary Controls:

1) Validity and integrity controls: The validity and integrity of data taken by telephone, voice mail, letter or e-mail produced outside the organization shall be controlled appropriately without making a critic transaction on the datum.

2) Protection of sensitive information during transmission and transfer: Sensitive information shall be protected during transmission and transfer against unauthorized access, change and rerouting.

(4) The auditor shall consider

a) The definition of important application components and the flow of transactions over the system, inspection of current documentation and understanding the details of applications by contacting the related personnel,

b) The definition of the strong aspect of the application controls and the evaluation of the effect of control weaknesses to the test strategy by analyzing collected information,

c) Testing the functionality and efficiency of controls by using appropriate audit procedures,

d) Analyzing the test results and other audit findings as well as the evaluation of control environment.

(5) Application controls minimally include the audit and evaluation activities on the areas below;

a) Analyzing the existence of double information systems and double accounting systems and the prevention of them,

b) Preparing the interest and income realization calculations, expense rediscounts and amortization calculations, prosecution calculations and provision calculations, aging report.

c) Forming the balance by the process of determining and authorizing the responsible personnel for giving accounting check, the existence of authorizations related to the retrospective transactions of giving accounting check and the integrity and traceability of related recordings, general accounting controls such as providing the sequentiality of transaction number, transaction limits and authorization control.

d) Electronic Fund Transfer, Electronic Security Transfer and Clearing Bank transactions, SWIFT transactions and security records thereof such as payment system controls.

e) Agreement controls such as agreements relating to nostro, vostro and loro balances, agreements between recordings of branches and general management, agreements between legal and companion books, agreements of bank and card centers,

f) Controls relating to the applications such as the limit allocation to the bank and credit card, usage of bankcards and gift points,

g) Controls relating to the credit applications and approvals, credit limits as well as back payment statements of credits and calculation of them; counting and controls such as deposit transactions and deposit classification,

h) Controls of the usage process of bank recordings and information sources in financial reporting,

i) Control of security and fund management

j) Control of reliability and integrity of recordings related to the maturity and value dates,

k) Controls of accounting and process related to the electronic banking/alternative distribution channels (Internet, telephone, television, WAP/GPRS, Kiosk, ATM, etc.)

(6) Auditors evaluate the adequacy of the internal controls on the financial reporting system of the banks and the performance of the directors on the measurement of adequacy and efficiency of these internal controls as well as the application controls. The issues they evaluate under this evaluation are as follows;

a) In the process of auditing of internal control system;

1) Planning,

2) Reviewing the evaluation process on the internal control of management,

3) Forming the evaluation on the internal controls,

4) Testing the design of internal controls, evaluating the efficiency and adequacy of them,

5) Testing the application of internal controls, evaluating the efficiency and adequacy of them,

6) Forming the vision on the efficiency and effectiveness of internal controls,

b In the internal controls on financial reporting;

1) Control environment,

2) Risk evaluation process,

3) Control activities,

4) Information and interaction channels, authorization, recording processes,

5) Prosecuting Monitoring the controls formed by the audited institution.

Information criteria, technology resources and managerial criteria in the supervision of information systems

ARTICLE 19 – (1) Each control object realized in the scope of Articles 14, 15, 16 and 17 of this regulation is evaluated in compliance with the methods in the framework of The Control Objectives for Information and related Technology (COBIT) by considering the information criteria, technology resources and managerial criteria together in their applicability measure and maturity level for each audited process is determined. The existence, compliance and the support of managerial criteria is taken into consideration in the application of this provision

SECTION FIVE
General Principles and Responsibilities
Contract of information systems audit

ARTICLE 20 – (1) Information systems audit is carried out according to framework of the contract signed between the authorized institution and the audited institution. Contract of information systems supervision shows that there is a complete agreement between the sides on the scope and content of the information systems audit. Contract of information systems audit can be included in the contract made in the scope of Article 9 of RAIIA.

(2) Contracts of information systems audit come into force by the approval of the board of the audited institution. A copy of a contract by the audited institution is submitted to the Agency within 5 days as of the contracts being put into force.

(3) The authorized institution shall make the necessary pre-research in order to determine the scope and planning of information systems supervision before making audit contract with the audited institution. In the scope of pre-research, information shall be required on the issues that can affect the audit process positively or negatively and in the case of the change of authorized institution, the reasons of it from the institutions previously responsible from the audit. The audited institution shall inform the title of the contracted with for the current period to the authorized institution that had been previously responsible for the audit and it shall be authorized to give the information required. The institution which was previously responsible for the supervision should give the information required in this scope.

(4) The issues, which have to be in the Contract of information systems audit, are as follows;

a) The regulations that the auditor is liable to obey,

b) The aim, scope and reasons of the information systems supervision,

c) The services rendered by the authorized institution in the scope of the contract.

d) The responsibilities and liabilities of the sides,

e) The supervisors being authorized in the audit and the reserve of them,

f) The titles of the person auditors assigned in the audit team, the previewed working periods and the detailed document of the charge found appropriate for each.

g) The starting date and completion date of the audit.

h) The form of the information systems supervision report as well as the form of the special purpose audit report and the reasons of the preparation of these reports,

i) The deadline of the report.

(5) The audited institution can void the contract by setting forth the ground that they act contrary to the contract of supervision of information systems and the supervision is not done appropriate to the principles, and this situation shall be informed to the agency within five days.

(6) The audit may be abrogated in case of limiting significantly the auditor's sphere of performance contrary to the provisions of the contract, not being able to acquire the information and documents relating to information systems or in case of the situation similar to thereof arising, provided that making out a written statement and having a notice in advance to the Agency. The authorized institution declares the situation and reasons thereof to the Agency immediately with the withdrawing from the audit justifications. In case of withdrawal, it is compulsory that, the authorized institution shall transmit all working sheets and information required to the Agency with a view to transfer thereof to the replaced authorized institution. It is compulsory that, the institution authorized, which shall be replaced to the institution withdrawn, be deemed appropriate by the Agency.

(7) The auditor provides provisions procuring to hold a meeting and conversation relating to auditing respects with the support service institution in case that the party under audit executes certain activities by support service institution.

Informing Administrators

ARTICLE 21 – (1) If it is determined that the party under audit have significant weakness on its information system on account of not forming appropriate controls to important risks concerning information systems, the auditor informs the Agency and the managers of the party under audit concerning the state immediately and takes into consideration the effect of the state thereof in risk evaluation.

Documentation

ARTICLE 22 – (1) The auditor documents the respects hereunder;

a) Evaluations concerning the sensibility to declaration risk of the party under audit due to mistakes or abuse in information systems and financial data production processes and the important decisions reached.

b) The essential factors and resources of the information concerning the environment audited and the risk evaluation techniques, including the environment of control, whether the party under audit’s having adequate and regular risk measurement, control and management techniques or not, data processing system, activities of control and monitoring of controls

c) Risks determined and the controls concerned.

SECTION SIX

Outsourcing of the Party under Audit and Auditing Thereof

Outsourced Services of the Party under Audit

ARTICLE 23 – (1) The auditor, takes into consideration that how the outsourced services by outsourcing of the party under audit affect information systems and financial data production processes; plans the information system audit according to thereof and develops an efficient audit approach.

Information System Audit Report of the Outsourced Institution

ARTICLE 24 – (1) The auditor may demand the information systems audit report which was prepared relevant to outsourced institution and analyses the professional expertise of information systems auditor who audits the outsourced institution, the structure of the report, content, utilization and adequacy of thereof and evaluates herewith. The authorized institution takes into consideration of the scope of information systems audit made by the auditor auditing the outsourced institution.

(2) When the auditor uses information systems audit which was prepared for the support service institution, the auditor shall not indicate reference to the report thereof within his own report, which the auditor prepares.

SECTION SEVEN
Cooperation in Information Systems Audit
Cooperation in between the Auditors

ARTICLE 25 – (1) The authorized institution and the auditor executed the preceding information system audit are obliged to provide all sorts of information and documents which constituting basis to information systems audit, within the scope of confidentiality principle, to the institutions and entities which shall made the information systems audit.

(2) Entities, responsible from the activities of internal control and internal auditor of the party under audit, transmit all information required, including their own reports, to information systems auditors.

(3) Dependent on the auditor’s conviction relevant to the party under audit’s internal control and risk management system adequacy,; it is shown care that the party under audit should avoid repetition in internal audit activities and information systems audit activities as much as possible.

Cooperation in between the Agency and the Institutions Authorized

ARTICLE 26 – (1) Meetings may be arranged in between the Agency and the institutions authorized and auditors for exchanging ideas and information in respects of common sphere of interests. It can be make an attempt on this respect by the Agency or the auditors.

(2) The information provided in information system auditing activities made by the Agency in banks shall be shared out with the auditors when needed.

(3) The personnel of the Agency shall attend all stages of information systems auditing process of the institutions authorized by observer status, with a view to develop the information and skill, without injuring auditor independency principle. The personnel of the Agency shall not utilize the knowledge of the authorized institution for personal use or drawing benefit for any other authorized institution. The authorized institution makes an effort and contribution required in order that the personnel of the Agency shall be included in the process and shall increase their knowledge.

(4) The auditors and the authorized institutions shall declare the important information like hereunder which shall concern the Agency and which shall necessitate taking action urgently on behalf of the Agency;

a) The facts that shall jeopardize the subsistence of a bank,

b) The probability of fraud in which the information systems are used as instrument,

c) Information system auditor’s having an intention of abdication,

d) The activity risks of the Bank’s or probable risks’ increasing,

e) Significant defects on control environment,

f) Information revealing that the bank did not fulfill one of the criteria for carrying on banking authority,

g) Information that shall or may affect significantly the financial state of the bank,

h) Information that shall or may have significant affect on administrative and internal control of the bank such as a serious conflict with resolution organs, an unexpected severance of a key manager,

i) Information revealing that the laws, regulations, main agreement or statute of which the party under audit is subject to were contravened,

j) Important defects and risks included within the information systems.

SECTION EIGHT

Outsourcing of Information systems Auditing

Fulfillment the information system auditing by receiving external service

ARTICLE 27 – (1) Independent Audit Institution can realize the information system auditing by outsourcing by taking into consideration of the activity structure of the party under audit. In order that the external service provider shall realize the information system auditing of the institution, within the scope of the Regulation thereof; it must make a contract with the independent audit institution. With the contract thereof, the independent audit institution shall provide that the external service provider institution shall comply with the auditing principles of the institution, shall support all terms regulated for the auditors within the scope of the Regulation thereof and other regulations concerned and shall comply with the articles concerned.

(2) The auditor of the external service provider institutions

a) possessing the auditor qualities determined within the Regulation thereof,

b) An adequate number of auditors' being employed within the information system auditing team,

c) Not furnishing advisory and management service to the institution under audit minimum within the last three years and not having a commercial relation herewith,

d) The auditors' being dependent on auditing principles and being assigned in information system auditing provided that the auditors not harm the auditor independency of the external service provider institutions is obligatory

(3) The contract, which is planned to be made in between the independent audit institution and external service provider institution, is transmitted to the Agency and to the bank to be audited before the auditing study initiates and it is reached to a mutual agreement. The authorized institution is obliged to make an amendment required on the contract and transmit thereof for taking the mutual understanding to the Agency and to the party under audit in five business days in case that it realizes the need of receiving external service in information systems auditing after the auditing activities.

(4) In case that the contract of the external service provider institution is abolished or withdrawn from the audit within the contractual period, the independent audit institution is obligatory to declare the state to the Agency with the justification.

(5) The independent audit institution's making contract with an external service provider institution does not mean that the independent audit institution is transferring the responsibilities.

(6) The independent audit institution monitors the performance of the external service provider institution and the changes in qualities that it has to provide during agreement period. The independent audit institution must evaluate service level agreements, internal control mechanisms, auditing and financial reporting of external service provider

(7) The independent audit institution may receive external service more than one external service provider institution, provided that it shall be conformed to the respects written in the article, in consideration that the area of specialization showing dissimilarity.

(8) The external service provider institution realize the information systems audit within the scope of this Regulation and signs the information systems audit report with the independent audit institution pursuant to the respects declared within the Regulation. The external service provider institution must mention the entity that it gave the authorization to sign the audit report explicitly within the contract.

(9) The external service provider institution is examined on-site, concerning the determination of the professional and technical adequacy, by the Agency.

(10) An external service provider institution shall not furnish a service of information system auditing to the same bank consequently more than seven years.

SECTION NINE
Information Systems Auditing Report and Declaration

Information Systems Auditing Report

ARTICLE 28 – (1) By taking into consideration of the materiality concept, information systems auditing report is a text on which the conviction of the information systems auditor was revealed by a clear language in written, and in which the evaluation of information systems and financial data production process are included. The duty of the auditor are, collecting evidences of audit concerning application controls and general controls and analyzing and evaluating thereof and developing conviction regarding information system auditing by reaching a conclusion upon the evidences thereof.

(2) The auditor must arrange information systems auditing report after the auditing studies. The basis and procedures relevant to the report are arranged by the communiqué that shall be published by the Board.

(3) Information systems auditing report includes all the activities belonging to the period on which the information systems auditing was realized. If the reports accomplished are signed by responsible information system head auditor of the authorized institution or if the audit conducted by means of outsourcing of information systems auditing, they are signed by the authorized person of the firm concerned and in both cases by common responsible executive auditor determined in RAIIA. In case that the authorized institution charge a responsible partner head auditor having the required qualifications defined in the regulation herein with executing information systems auditing, the independent audit report shall be signed by, instead of responsible information systems head auditor, other responsible partner head auditor and the person thereof.

(4) Information systems auditing report, unless otherwise specified by the Board, is accomplished within the first month of the year following the auditing period and is transmitted to the presidency of the board of directors, audit committee, the CBRT and to the Agency as three copies in the annex holding the signature of the entities having the authority to bind and to represent the authorized institution. The

copy of information systems audit report in electronic media which was signed with secure electronic signature pursuant to the provisions of the Law Dated January 15, 2004, Nr. 5070 on Electronic Signature Law is also transmitted to the Agency. The Agency can predict the said report to be transmitted with the independent audit report when considered necessary.

(5) The content of the information systems report is confidential information and shall not be published in any media. The secrecy and safety of the information thereof is under the accountability of the BRSA, CBRT, the institutions authorized, the independent audit institutions within the scope of the Regulation thereof, the external service provider institutions and the party under audit. The parties under audit shall not make a statement including the audit conclusions and shall not use the respects thereof with a view to advertise.

SECTION TEN

Various and the Last Provisions

Serving in the Banks of Information Systems Auditors

ARTICLE 29 – (1) The auditors shall not be employed in the banks to which they participated to the auditing process in last two years.

The situations that were not provisioned in the Regulation

ARTICLE 30 – (1) For the situations that were not provisioned in the Regulation; procedures and principles included in the documents of COBIT (Control Objectives for Information Technologies) which was published by Information Technologies Governance Institution (ITGI) and Information Systems Audit Control Agency (ISACA) that offering internationally accepted information technologies control objectives and the norms that EU regulations has brought are applied.

Auditing the institutions within the scope of consolidation

PROVISIONAL ARTICLE 1 – (1) The audit of the institutions within the scope of consolidation with the banks within the framework of the provisions of this Regulation is initiated by January 01, 2007.

Signature Obligation

PROVISIONAL ARTICLE 2 – (1) It is obligatory that the contracts relating to information systems audit to be realized for the year 2006 shall be signed within three months as of the publication of this Regulation Agency may prolong the deadline as it deems necessary

Enforcement

ARTICLE 31 – (1) This regulation enters into force in the publication date.

Execution

ARTICLE 32 – (1) The Chairman of the Agency executes the provisions of the Regulation.