REGULATION ON AUDIT OF BANK INFORMATION SYSTEMS AND BANKING PROCESSES TO BE CONDUCTED BY INDEPENDENT AUDIT FIRMS

FIRST PART
Purpose, Scope, Grounds, Definitions and Abbreviations

Purpose:

ARTICLE 1 – (1) The purpose of this Regulation is to set down the procedures and principles and the terms and conditions regarding audit of information systems and banking processes of banks by the authorized independent audit firms.

Scope:

ARTICLE 2 – (1) Banks, and their consolidated affiliates and subsidiaries solely for the purpose of issuance of a report on audit of information systems and banking processes of banks, and support service providers offering information systems services to banks, and firms authorized to audit information systems and banking processes, and independent audit firms and external service providers are covered and governed by the provisions of this Regulation solely for the specific purpose set down in the preceding Article 1.

Grounds:

ARTICLE 3 – (1) This Regulation has been prepared and issued in reliance upon provisions of Article 15 and fourth paragraph of Article 93 of the Banking Law no. 5411 dated 19/10/2005.

Definitions and Abbreviations:

ARTICLE 4 – (1) For the purposes and in the context of this Regulation:

a) "Independent audit" shall have the meaning ascribed thereto in first paragraph of Article 5 of the Regulation on Authorization and Activities of Firms to Conduct Independent Audit on Banks, promulgated in the Official Gazette edition 26333 on 1/11/2006; and

b) "Independent audit firm" refers to a firm authorized to conduct independent audit on banks according to Article 18 of the Regulation on

Authorization and Activities of Firms to Conduct Independent Audit on Banks; and

c) "Bank" shall have the meaning ascribed thereto in Article 3 of the Law; and

ç) "Banking processes" refers to the business processes established in respect of the activities conducted by the auditee within the frame of Article 4 of the Law; and

d) "BDYFY" refers to and stands for the Regulation on Authorization and Activities of Firms to Conduct Independent Audit on Banks, promulgated in the Official Gazette edition 26333 on 1/11/2006; and

e) "BSD" refers to and stands for the audit on information systems and banking processes of banks; and

f) **(Amended by the Regulation promulgated in the Official Gazette edition 28896 on 28/1/2014)** "COBIT" refers to and stands for the version deemed fit by the Agency as of the beginning of audit period of the Control Objectives for Information Technologies (COBIT) published by Information Systems Audit and Control Association (ISACA) Information Technologies Governance Institute (ITGI); and

g) "Auditor" refers to both personnel who are assigned by the authorized firm for performance of audit on information systems and banking processes and the job titles of whom are listed in Article 18 of this Regulation, and financial auditor involved in banking processes audit activities; and

ğ) "Auditee" refers to banks, and their consolidated affiliates and subsidiaries solely for the purpose of issuance of a report on audit of information systems and banking processes of banks, and their support service providers; and

h) "Financial auditor" refers to an independent auditor as defined in Article 4 of BDYFY; and

ı) "General controls" refers to the controls applied on all or a great part of bank information systems and aiming to provide an adequate assurance in respect of correct performance of the functions expected from information systems and prevention, determination and correction of undesired events, and to establish a reliable environment for the sake of functionality of

controls on banking processes, as well as the policies and procedures ensuring application of these controls; and

i) "Law" refers to and stands for the Banking Law no. 5411; and

j) "Control" refers to all of policies, procedures, applications and organizational structures aiming to provide an adequate assurance in respect of achievement of business objectives and prevention, determination and correction of undesired events; and

k) "Control objectives" refers to control objectives mentioned in COBIT aiming to ensure achievement of a desired consequence or purpose by building control procedures within a certain information systems activity; and

l) "Board" refers to and stands for the Banking Regulation and Supervision Board; and

m) "Agency" refers to and stands for the Banking Regulation and Supervision Agency; and

n) "Maturity model" refers to a maturity model as described in COBIT; and

o) "Authorized firm" refers to an independent audit firm authorized to conduct audit pursuant to and under this Regulation; and

ö) "Managers" refers to the managers as defined in Article 3 of the Law.

SECOND PART
General Concepts on Audit of Information Systems and Banking Processes

Materiality:

ARTICLE 5 – (1) Materiality is a subject of opinion based upon professional experience, and means the assessment of actual or potential effects of errors, omissions, breaches of procedures, and unlawful acts that emerge or may emerge as a result of control weaknesses on reporting of financial data by banks and on provision of secure and uninterrupted services by banks.

(2) In audit of information systems and banking processes, the materiality concept may be used for planning of audit, and intensification of audit on the required areas, and assessment and reporting of findings.

(3) Integrity, consistency, reliability, and if needed, confidentiality of data considered as sensitive on the part of the auditee, particularly financial data, as well as continuity of activities are the basic components required to be taken into consideration as a part of the materiality concept.

(4) In assessment of controls affecting financial reports, such components as value of financial transaction carried out by the process or system, and frequency of transaction are used, while in assessment of controls unrelated to financial transactions, such components as criticality of business process, cost of systems and operations, size of potential consequences of errors, number of transactions/inquiries executed within a certain time interval, nature, description, timing and scope of files kept and reports issued, requirements of service level agreements, and amounts of fines in penal clauses are used.

Control Weakness:

ARTICLE 6 – (1) Auditor uses the following criteria in classification of control weaknesses and deficiencies covered by findings reached as a result of its inspections and examinations according to the materiality concept:

a) Control weakness: Refers to failure of design or operation of a control in prevention and detection of errors in a timely fashion.

1) Control deficiency in design refers to non-availability of a control as needed for achievement of a control objective, or failure of an existing control in achievement of control objective expected from it due to mistakes in its design though it is operating and running as designed.

2) Control deficiency in operation refers to failure of a well-designed control in operation as designed, or lack of authorization and competence of control personnel as required for effective performance of control.

b) Considerable control deficiency: Refers to a deficiency not considerable immaterial which emerges as a result of a control weakness or several control weaknesses that may make a negative effect on ensuring the integrity, consistency, reliability, and if and when needed, confidentiality of financial data of the auditee, and on assurance of continuity of its activities.

Deficiencies which may probably make a negative effect on prevention of errors and omissions occurring during recording of financial data of the auditee reliably in accordance with the generally accepted accounting standards, and during authorization, processing or reporting of the records are also considered and treated in this category.

c) Major control deficiency: Refers to a control deficiency or a combination of several control deficiencies which may hinder or obstruct the prevention or correction of a material mistake in periodical financial reporting of the auditee, or may most probably make a material negative effect on ensuring the integrity, consistency, reliability, continuity, and if and when needed, confidentiality of the processes conducted within the bank organization and of the information pertaining to those processes.

Efficiency, Adequacy and Compatibility:

ARTICLE 7 – (1) In order for design of a control to be accepted as efficient, a control deficiency in design should not exist in this control, or even if existing, should not lead to a major control deficiency.

(2) In order for operation of a control to be accepted as efficient, a control deficiency in operation should not exist in this control, or even if existing, should not lead to a major control deficiency.

(3) Adequacy of controls on information systems and banking processes means:

a) that designs of all controls subject to audit within the frame of the materiality principle are efficient and effective; and

b) that these controls are designed so as to be capable of generating the consequences expected from them within the frame of business objectives and compensating the probable risk exposures.

(4) Efficiency of controls on information systems and banking processes means:

a) that operation of all controls subject to audit within the frame of the materiality principle is efficient and effective; and

b) that these controls are capable of properly performing all functions expected from them and achieving the control objectives.

(5) A control may be deemed to be compatible only if and when all of the requirements and obligations relating to that control as described in the Law and in the regulations and directives issued and published in reliance upon the Law are duly and fully satisfied and performed. Compatibility of controls on information systems and banking processes means that all controls subject to audit within the frame of the materiality principle are compatible.

Audit Risk:

ARTICLE 8 – (1) Audit risk refers to the probability of failure of an auditor to express correct opinions due to the following risks:

a) Structural risk: Refers to the risk of existence of at least a considerable control deficiency because of lack of control.

b) Control risk: Refers to the risk of failure of a control to prevent, detect or timely correct at least a considerable control deficiency due to its failure in proper running and operation.

c) Detection risk: Refers to the risk of failure of an auditor to detect and find out at least a considerable control deficiency existing in internal control system of the auditee.

(2) Major or considerable control deficiency risk: Refers to the risk of existence of at least a considerable control deficiency in internal control system of the auditee. Major or considerable control deficiency risk arises out of structural risk and control risk.

(3) In order to reduce the audit risk to a reasonable level, auditor uses and employs appropriate audit techniques capable of reducing the detection risk in areas where major or considerable control deficiency risk is high.

THIRD PART
Authorization, Permission and Professionals

Conditions Sought for in Firms to be Authorized:

ARTICLE 9 – (1) Firms to be authorized pursuant to and under this Regulation are required:

a) to have authorization to conduct independent audit on banks, and

b) to employ auditors of an adequate number and adequate qualifications for performance of activities covered by this Regulation.

Information and Documents Requested to be Submitted in Application for Authorization:

ARTICLE 10 – (1) A petition of application to be submitted to the Agency by an independent audit firm wishing to engage in BSD activities will be accompanied by the following submittals regarding all auditors other than assistant auditors:

a) Detailed curriculum vitae to be issued in accordance with the format given in Exhibit-1 attached hereto and containing information about their professional experiences, audit-related trainings taken, and if any, audit works participated, and duties assumed in the course of those works, as well as original or an Agency-certified copy of their diplomas / certificates of graduation relating to undergraduate and postgraduate educations; and

b) If any, original or an Agency-certified copy of their Certified Information Systems Auditor (CISA) certificate or other certificates relating to the scope of this Regulation; and

c) Copies of certificates relating to trainings given or taken on the issues with regard to the scope of this Regulation; and

ç) Their written statement that they do not have any past criminal records; and

d) Their job titles deemed fit and appropriate under this Regulation; and

e) Their written statement to be issued in accordance with the format given in Exhibit-2 attached hereto and certifying that they do not hold any partnership shares in more than one independent audit firm; and

f) Their written statement to be issued in accordance with the format given in Exhibit-3 attached hereto and certifying that they are not a partner in independent audit firms the authorization to conduct audit in auditees or companies subject to and governed by the Capital Markets Law no. 2499 dated 28/7/1981 of which has been cancelled, or they are not involved in an audit activity causing the cancellation of authorization as an independent auditor or an auditor; and

g) Their written statement to be issued in accordance with the format given in Exhibit-4 attached hereto and certifying that they do not work in any job other than their professional activities; and

ğ) Their written statement to be issued in accordance with the format given in Exhibit-5 attached hereto and certifying that they are working or will work on full-time basis in the independent audit firm; and

h) Providing that it is documented and proven by a certificate to be requested from the relevant entity that they have not ever been disqualified for independent audit activities as a result of a disciplinary proceeding conducted previously or to be conducted in the future, their written statement to be issued in accordance with the format given in Exhibit-6 attached hereto and declaring whether a disciplinary proceeding is conducted by other authorized institutions about them or not, and that if and when such a disciplinary proceeding is initiated, they are going to inform the Agency within maximum seven days, and that if, as a result of such disciplinary proceeding, they receive a punishment precluding them from audit of information systems, they are going to resign from their jobs within no later than fifteen days thereafter; and

ı) Their written letter of undertaking to be issued in accordance with the format given in Exhibit-7 attached hereto and certifying that if and when they lose their independence during their BSD activities, they agree and undertake in advance to resign from their audit services offered to the bank.

(2) The petition of application is also required to contain a statement of the independent audit firm that it is going to take out a professional liability insurance cover with a view to indemnifying all and any damages that may arise out of its services.

Grant of Authorization to Conduct Audit on Information Systems and Banking Processes:

ARTICLE 11 – (1) If and when partners and auditors of an independent audit firm filing an application for authorization to conduct audit on information systems and banking processes are assessed in the light of the information and documents referred to in Article 10 of this Regulation, and as a result of an onsite examination conducted by the Agency for the purpose of determination of their professional and technical competences and qualifications, if it is concluded that said partners and auditors are adequately qualified and competent for conduct of their fields of activity, then and in this case, said authorized firm is granted the authorization to

conduct audit on banks pursuant to and under this Regulation by a decision of the Board.

(2) In the course of process of assessment of applications for authorization, if and when deemed necessary by the Agency, additional information and documents may be requested for the purpose of measurement of competency and adequacy of subject independent audit firm. Information and documents requested as such are also taken into account in assessments relating to grant of authorization.

(3) Issues and points taken into consideration in the process of authorization of independent audit firms may be reviewed by the Agency.

(4) Factors paving the way for grant of an authorization of audit under this Regulation are essentially required to be satisfied continuously. The Agency may at any time considered fit and necessary check the existence of these components.

(5) Titles of independent audit firms authorized to conduct audits pursuant to and under this Regulation are published in the Agency's internet site.

Withdrawal of Authorization to Conduct Audit on Information Systems and Banking Processes:

ARTICLE 12 – (1) Upon occurrence of any of the following events, the authorization of authorized firm to conduct audit on information systems and banking processes is permanently removed and withdrawn by the Board:

a) Performance of the activities of audit on information systems and banking processes in conflict with the provisions of third paragraph of Article 26 of BDYFY; or

b) Failure in taking out the professional liability insurance which is mandatorily required to be purchased pursuant to Article 36 of the Law and within the frame of procedures and principles set down in eleventh and twelfth paragraphs of Article 26 of BDYFY, in such manner to cover also the audit of information systems and banking processes, for more than once; or

c) If and when the Agency finds out any events or factors which may effect to the extent of materiality the capability of information systems and banking processes and systems, which have received a positive unqualified

opinion, a qualified opinion or an adverse opinion, to ensure protection of assets of the auditee, and performance of its activities effectively, efficiently and in accordance with the Law and other applicable laws and regulations, and bank's internal policies and rules, and banking usage and practices, and reliability and integrity of accounting and financial reporting system, and timely availability of information, then and in this case, failure of the authorized firm in proving and demonstrating that it is not culpable and blameable in connection therewith; or

ç) Temporary withdrawal of authorization for more than once as per the second paragraph hereinbelow; or

d) Non-availability of a continuing audit contract as required under this Regulation, or as shown by audits, failure in satisfaction of the conditions set down in audit contract at all or completely; or

e) Contradiction with provisions of eleventh paragraph of Article 20 hereof; or

f) Loss by the authorized firm of the conditions and qualifications set down in Article 9 hereinabove.

(2) Upon occurrence of any one or more of the following events, the Board is authorized to remove and withdraw temporarily for a maximum period of two years the authorization of the authorized firm to conduct audit on information systems and banking processes of banks:

a) Contradiction of job titles used by auditors with provisions of Article 18 hereof; or

b) Replacement of auditors without a prior notice to the auditees and to the Agency; or

c) **(Repealed by the Regulation promulgated in the Official Gazette edition 28006 on 26/7/2011)**; or

ç) Failure to obtain adequate audit evidences; or

d) Failure in provision of the information and documents requested by the Agency.

(3) Defence of the relevant authorization firm is taken before temporary or permanent removal or withdrawal of authorization. If an authorized firm fails

to give a defence within one month following the date of delivery of the notice of request of defence, it will be deemed to have waived from its right of defence.

(4) Withdrawal of authorization of an authorized firm to conduct audits pursuant to and under this Regulation does, however, not construe as withdrawal of its authorization to conduct independent audit. On the other hand, if and when the authorization of an authorized firm to conduct independent audit is withdrawn, its authorization to conduct audits pursuant to and under this Regulation is also deemed to have been removed and withdrawn automatically without any further act.

(5) The Board prohibits the partners or auditors of an authorized firm who are determined to be responsible for non-compliance with warnings made by the Agency or for repetition of the acts, being the subject of said warnings, or who do not perform the obligations set down in Article 20 hereinbelow, to engage in BSD activities by using their professional job titles as defined in Article 18 of this Regulation.

(6) Titles of independent audit firms the authorization to conduct audit of which is withdrawn and removed under this Regulation are also published in the Agency's internet site.

Performance of Audit on Bank Information Systems and Banking Processes Through Outsourcing:

ARTICLE 13 – (1) Independent audit firm may perform its BSD activities through outsourcing.

(2) Independent audit firm is under obligation to get a prior permission under this Regulation in order to perform its BSD activities on the auditee through services to be outsourced to external service provider/providers.

(3) Also in case of performance of audit activities through outsourcing. Independent audit firm is finally and personally responsible both in its own name and in the name of external service provider/providers assigned by it, for the related activities and for performance of its obligations arising out of this Regulation.

(4) The same external service provider may offer its services to more than one independent audit firm.

(5) An independent audit firm may file an application for permission to conduct BSD activities through outsourcing for not more than 3 periods at one time. Upon expiration of period of permission, the related independent audit firm is allowed to re-apply for permission to conduct audit activities through outsourcing.

Conditions Sought for in External Service Provider:

ARTICLE 14 – (1) External service providers from which independent audit firm may receive services for conduct of its BSD activities are required to comply with the following conditions:

a) Its auditor must have the auditor qualifications defined and described in this Regulation; and

b) It must employ auditors of adequate number and adequate qualities in its audit teams; and

c) It should not have given management and consulting services to and should not have entered into any commercial relationship with the auditee since the last three years at the minimum; and

ç) Its auditor must take part in audit of information systems and banking processes, providing that all audit principles are complied with, and the auditor's independence principle is not breached; and

d) It should not have conducted audit on the same auditee continuously for 7 years or a longer period under this Regulation.

(2) In order to be eligible for performance of audit on information systems and banking processes, the external service provider must have entered into an agreement with independent audit firm pursuant to and under this Regulation. By said agreement, independent audit firm is obligated to make sure that the external service provider remains bound by audit principles, and meets and satisfies all conditions sought for in auditors as per this Regulation and other relevant regulations, and complies with the provisions pertaining to audit activities and other related issues.

Information and Documents Requested to be Submitted in Application for Permission:

ARTICLE 15 – (1) An independent audit firm wishing to conduct its BST activities through outsourcing is required to clearly state the identity of

auditees to be audited by it and the audit periods in its petition of application to be submitted to the Agency.

(2) Petition of application to be submitted to the Agency is required to be accompanied by the following information and documents:

a) A memorandum of understanding received from banks receiving independent audit services from the applicant and verifying that the subject external service provider is unobjectionably eligible for conduct of audit on information systems and banking process in the bank; and

b) Documents required to be submitted pursuant to first and second paragraphs of Article 10 hereof in respect of independent audit firm and external service provider and their partners and auditors; and

c) A contract signed between independent audit firm and external service provider, clearly setting down the mutual obligations of the parties thereto, as well as the audit plan, and giving information about the person assigned and authorized by external service provider to sign the audit report, as well as audit principles, audit/auditor independence, confidentiality and conflict of interests, audit teams, hourly audit fee and total service fee; and

ç) Addresses of head offices and if any, branch and/or branches of external service provider; and

d) Balance sheet of external service provider issued as of the date of balance sheet; and

e) If external service provider has a legal relationship with a foreign company with regard to the area of outsourcing, a copy certified by the duly authorized officers of the company of the agreements signed with that company; and

f) Written statements issued in accordance with the format shown in Exhibit-8 attached hereto by external service provider and certifying that it has not ever given any management and counselling services to and has not entered into any commercial relations with the auditee or to its affiliates or subsidiaries since the last three years at the minimum; and

g) Written statements issued in accordance with the format shown in Exhibit-9 attached hereto by auditors of external service provider and certifying that they accept to be involved in audit of information systems and

banking processes, providing that audit principles are complied with, and confidentiality and auditor independence principles are not impaired.

Grant of Permission to Conduct Audit on Information Systems and Banking Processes Through Outsourcing:

ARTICLE 16 – (1) If and when independent audit firms and external service providers and their partners and auditors filing an application for permission to conduct BSD through outsourcing are assessed in the light of the information and documents referred to in Article 10 of this Regulation, and as a result of an onsite examination conducted by the Agency for the purpose of determination of their professional and technical competences and qualifications, if it is concluded that said independent audit firms and external service providers and their partners and auditors are adequately qualified and competent for conduct of their fields of activity, then and in this case, they are granted the permission to conduct BSD on auditees pursuant to and under this Regulation by a decision of the Board.

(2) If external service provider chosen by independent audit firm is an authorized firm under this Regulation, a Board decision is not sought for, but the Agency's assessments are relied upon in respect of, permission to conduct BSD through outsourcing.

(3) Where external service provider is an authorized firm, in assessments to be made by the Agency, the adequacy of sources owned and possessed by the firm for subject services and for audit activities presently carried out under this Regulation is to be taken into account.

(4) Independent audit firms getting a permission to conduct audits through outsourcing, and solely for their services offered within the frame of BSD, the relevant external service providers are, unless otherwise stated, subject to and governed by all provisions of this Regulation pertaining to authorized firms.

Cancellation of Permission to Conduct Audit on Information Systems and Banking Processes Through Outsourcing:

ARTICLE 17 – (1) In case of detection of any one or more of the events specified in first and second paragraphs of Article 12 in the authorized firms and their external service providers demonstrated to have violated the related provisions of this Regulation, depending on the kind and nature of violations, and upon an assessment made by the Agency, the Board cancels and removes temporarily or permanently the permission of the relevant

independent audit firm to conduct audit on information systems and banking processes through outsourcing.

(2) Upon termination of the agreement between an independent audit firm and its external service provider, its permission to conduct BSD is also removed and withdrawn by the Board.

Job Titles of Professionals:

ARTICLE 18 – (1) Auditors get the job titles of responsible information systems lead independent auditor, information systems lead independent auditor, senior information systems independent auditor, information systems independent auditor, and information systems independent auditor assistant depending on their order of precedence and seniority.

(2) Total sum of periods actually spent in any one or more of information systems audit, professional information systems control or security, and software development areas and fields solely in respect of banking activities and operations will be accepted and treated as past professional experience pursuant to and under this Regulation.

(3) Total past job experience of financial auditors holding a Certified Information Systems Auditor (CISA) certificate is to be accepted and treated as past professional experience.

(4) In assessment of professional experience conditions, a portion of maximum 5 years of the past job experience, other than information systems audit also including third paragraph of this Article, will be deemed valid and acceptable. Each of Certified Information Systems Auditor (CISA) certificate and Certified Internal Auditor (CIA) certificate is to be deemed as an additional one-year past job experience in information systems audit in the course of assessment of professional experience conditions.

(5) Information Systems Independent Auditor is under obligation to meet and satisfy the following conditions:

a) To have completed 4-years' undergraduate programs of universities or foreign higher education institutions accepted by official authorities to be equivalent; and

b) To have a minimum 3 years of past professional experience.

(6) Senior Information Systems Independent Auditor is under obligation to meet and satisfy the following conditions:

a) To meet the conditions and qualifications sought for holding the job title of Information Systems Independent Auditor; and

b) To have a minimum 6 years of past professional experience.

(7) Information Systems Independent Lead Auditor is under obligation to meet and satisfy the following conditions:

a) To meet the conditions and qualifications sought for holding the job title of Information Systems Independent Auditor; and

b) To have a minimum 10 years of past professional experience; and

c) To hold a CISA certificate.

(8) Professionals meeting the conditions cited in seventh paragraph are granted the job title of Information Systems Independent Lead Auditor, if they are deemed eligible and qualified as a result of assessments made by the Agency.

(9) Promotions to professional job titles, other than Information Systems Independent Lead Auditor, are made by official authorities, and reported to the Agency in accordance with the procedures and principles determined by the Agency. Professionals who do not have knowledge, skills and merits (qualifications) sought for the next higher seniority cannot be promoted to the next higher job title even if they meet the past job experience condition.

(10) All of the professionals of authorized firms assigned and appointed for audit duties under this Regulation are under obligation to take or give continuous training in information systems and banking processes audit areas for at least twenty hours a year and for at least one hundred and twenty hours in three years.

FOURTH PART
Obligations of Parties

Obligations of Auditee:

ARTICLE 19 – (1) Auditee is under obligation to make its information systems documentation, documentation relating to banking processes, and

all kinds of records, information, documents, structures and systems pertaining to said documentations ready and convenient for audit hereunder.

(2) Auditee is obligated to disclose and furnish all kinds of information and documents, even if confidential, requested by the auditor for BSD purposes.

(3) Auditee is liable to report to auditors all of its systems and applications to be used in their audit works and activities together with a list of applications covering their purposes of use, and to present its work flow diagrams, documentation of control mechanisms, and user documents relating to banking applications, as prepared pursuant to and under Article 9 of the Regulation on Internal Systems of Banks promulgated in the Official Gazette edition 26333 on 1/11/2006.

(4) Auditee provides auditor with a copy of all internal audit reports requested by auditor, and takes necessary actions and measures for the sake of cooperation between auditor and auditee's inspectors as per Article 37 hereinbelow, and ensures that its inspectors respond and clarify in a timely fashion all questions directed by auditors of the authorized firm.

(5) Information of bank's board of directors about findings of auditors, and coordination between independent auditors on one side and directors and other personnel of auditee on the other side will be under responsibility of bank's audit committee.

(6) Where auditee requests change and replacement of contracted authorized firm at any time during the term of contract, or the authorized firm acts in contradiction with BSD agreement and/or does not conduct its audit in accordance with the principles set forth in this Regulation, this event is required to be notified to the Agency, together with reasons thereof, and a prior consent of the Board is required to be taken for termination of audit agreement.

(7) Auditee is obligated to provide auditor with a management statement approved by its board of directors and giving assurance about its internal controls as of the relevant audit period.

(8) Auditee issues an action plan containing its commitments in respect of solutions proposed for the findings put forth in its audit report, and reports the same in accordance with the procedures and principles to be determined by the Agency. Bank board of directors is liable for conduct of action plan

and for timely and complete performance of commitments contained in the action plan.

Obligations of Authorized Firms and Auditors:

ARTICLE 20 – (1) Auditors and financial auditors cooperating with auditors in BSD activities are under obligation to comply with their mandatory professional rules and principles and the audit principles cited in this Regulation and in BDYFY, and to prepare an audit plan by taking into consideration the probable risks and weaknesses that may be embedded in information systems and banking processes and within the frame of the professional scepticism, and to present and implement the audit plan to auditee, and not to accept and take the statements of directors as adequate audit evidences, and to create and issue audit report.

(2) Quality assurance system required to be established by independent audit firms in accordance with Article 13 of BDYFY is managed and handled in such manner to cover also audit works carried out and audit reports issued under this Regulation.

(3) Auditor is under obligation to give information about the detected errors, faults and misconducts in writing to auditee's directors and auditee's audit committee at each stage of the process.

(4) Changes or modifications in documents and statements mentioned in Article 10 of this Regulation are required to be notified to the Agency within seven days. Changes in audit staff are also notified to the Agency, together with reasons thereof, in accordance with the procedures and principles determined by the Agency.

(5) Authorized firms are under obligation to assure continuous participation of information systems auditors employed by them to training programs.

(6) If authorized firm reneges on BSD agreement or the agreement is terminated at any time during the term of agreement, authorized firm is under obligation to inform the Agency of such event, together with reasons thereof, within five business days thereafter.

(7) If, during BSD activities, any transactions which are in conflict with the basic provisions of applicable laws and regulations, or any incidents or developments which may lead to expression of a negative opinion or non-expression of an opinion are detected, even if auditee has resolved and

remedied these incidents or events, the Agency is required to be informed thereabout in writing by auditor within fifteen days after auditor becomes aware of them. In case of events which are categorized and considered as a crime according to the Law and other pertinent laws, the event is required to be urgently reported to the relevant official authorities, and the Agent is also separately informed thereabout in writing.

(8) Auditor immediately informs directors in writing or verbally about each matter or incident deemed important, including, but not limited to, the following events, detected during BSD activities:

a) Overall approach and scope of audit of information systems and banking processes, also including probable restrictions and additional works and activities; and

b) Problems relating to the policy-making process, or problems faced in policy applications, or changes in policy applications, which make or may make an important effect on information systems and banking processes; and

c) Uncertainties which may cast a doubt on continuity of banking activities; and

ç) Differences of opinion with directors on issues or matters which may make material effects on information systems and banking processes or on audit report; and

d) Material weaknesses and risks embedded in information systems and banking processes.

(9) In cases of verbal information, auditor documents the issues and events reported in working papers and the answers received in connection therewith.

(10) Auditors are under obligation to keep and maintain in good faith and without any modification all documentation and documents entrusted to them by the related persons within the frame of BSD activities until the end of time they are needed in the course of their business affairs, and to return and redeliver the same upon completion of the related works. Copies of the documents which constitute audit evidences may be kept by the authorized firm.

(11) Authorized firms and auditors are required to take all measures and actions needed for protection by them in strict confidence of all confidential information which come to their knowledge due to and in the course of their BSD activities and which are considered and treated as secrets according to the pertinent regulations and provisions, and cannot disclose such data and information to third parties, except for those who are legally authorized to receive the same, and cannot use such data and information directly or indirectly in their own interests.

(12) In the event that auditee fails to furnish information and documents pertaining to BSD activities to authorized firm, this event is promptly reported to the Agency.

(13) In case of change in auditors of authorized firms or employment of auditors other than assistant auditors, within no later than twenty days following the date of change or employment, both the documents of proof evidencing that these persons bear the conditions and qualifications sought for in the Regulation, and the copies of decisions relating to appointment or election of them are required to be delivered and submitted to the Agency in accordance with the procedures and principles determined by the Agency. Any such changes about which a negative opinion is not expressed within forty-five days as a result of assessment by the Agency are to be deemed valid and in force.

(14) Authorized firm is under obligation to take out a professional liability insurance having a coverage covering also the risks that may arise out of BSD activities.

(15) Authorized firm is obligated to furnish to the Agency upon demand or to present to the authorized audit professionals of the Agency all and any working papers to be issued by its auditors under and as per this Regulation, as well as all kinds of information and documents pertaining to audit.

FIFTH PART
Principles on Audit of Information Systems and Banking Processes

Audit of Information Systems and Banking Processes, and Purpose of Audit:

ARTICLE 21 – (1) BSD is a process comprised of the stages of assessment of elements of information system such as processes, activities, software and hardware covered by information systems management, and of processes

relating to banking activities, together with internal controls established within said systems and processes, followed by formulation of an opinion on the basis of assessment, and reporting of results thereof.

(2) Fundamental purpose of BSD is to formulate an opinion about compatibility, coherence, efficiency and adequacy of information systems and banking processes of auditee, and its internal controls pertaining to said systems and processes.

Scope of Audit of Information Systems and Banking Processes:

ARTICLE 22 – (1) Audit work to be performed pursuant to and under this Regulation is comprised of an audit of information systems as defined in Article 24 of this Regulation and an audit of banking processes again as defined in Article 25 hereof.

(2) Auditor determines in writing all processes, systems, activities and control mechanisms to be inspected within the bank information systems and banking processes with a risk-focused point of view and on the basis of materiality criterion. In addition, auditor makes sure that the scope of audits determined as above within the frame of materiality criterion is designed in such manner to obtain adequate audit evidences and proofs so as to provide a reasonable assurance for its audit opinion to be formulated and expressed under this Regulation.

(3) Activities conducted within the internal systems of auditee in respect of its internal control system are inspected under Article 26 hereinbelow and as a part of audit of banking processes.

(4) Audit of banking processes is conducted every year, while audit of information systems is repeated once every two years.

(5) The Agency may, if and when deemed necessary, differentiate scope and frequency of these audits for any one of auditees or for all auditees.

(6) Entities and institutions to be audited as a part of a consolidated BSD activity are determined in accordance with the provisions which are included in regulations issued by the Agency with regard to issuance of consolidated financial statements of banks and are taken into consideration in determination of institutions categorized as credit institutions or financial institutions to be covered by consolidated financial statements.

(7) Auditor determines in writing the scope of BSD to be performed on corporations required to be audited by it pursuant to sixth paragraph, by using materiality criteria, and in such manner to ensure determination of compatibility, coherence, efficiency and adequacy of controls on information systems and processes producing the financial data and information employed in consolidation.

Relationship between Independent Audit and Audit of Information Systems and Banking Processes:

ARTICLE 23 – (1) Independent audit and BSD activities are planned and implemented within a holistic and integrated approach, as they cover issues and points which may affect the scope and consequences of each other.

(2) In determining the scope of BSD and conducting its activities and works in connection therewith, auditor ensures not only the collection of adequate audit evidences for supporting its audit opinion, but also the collection of audit evidences for supporting the assessment of audit risks related to independent audit.

(3) Audit points and subjects mentioned in Article 35 of BDYFY are taken into consideration in the course of performance of activities covered by BSD, within the limits set forth in Article 22 of this Regulation.

(4) Where the opinion expressed on audit of information systems and banking processes is “qualified”, “negative” or “avoidance of expression of opinion”, both the opinion and the determinations and findings relied upon in the opinion are reported to financial auditor in writing.

Audit of Information Systems:

ARTICLE 24 – (1) Auditor inspects its general controls on information systems in terms of compatibility, coherence, efficiency and adequacy within the scope determined on the basis of materiality criterion.

(2) General controls are audited according to COBIT with regard to provisions of the regulations issued by the Agency in respect of principles to be employed in management of information systems in banks, independently from the framework, standards or methodologies used in establishment of these general controls.

(3) As a complementary element of the inspection works on compatibility, coherence, efficiency and adequacy of general controls, and within the frame

of maturity model, the maturity level of the process relating to the relevant control objective is also determined. In assessment of maturity level of the process relating to the relevant control objective, all of the detailed control objectives making up the process are taken into consideration and account.

Audit of Banking Processes:

ARTICLE 25 – (1) Auditor inspects banking processes of auditee and its internal controls on these processes in terms of compatibility, coherence, efficiency and adequacy within the scope determined on the basis of materiality criterion.

(2) As a part of audit of banking processes, all issues and matters relating to both the following processes concerning banking activities and other processes deemed fit and necessary are taken into consideration and assessed within the frame of materiality criterion:

a) Deposit Accounts Process: Transactions in relation to deposit accounts, and check/promissory note, fund transfer and collection transactions, and classification of deposits, and determination of scope of saving deposits, and calculation controls such as calculation of saving deposits insurance premiums, and controls regarding money laundering, and recognition of transactions, and other controls included in this process; and

b) Individual / Corporate Credit Facilities Process: Receipt and evaluation of credit requests and applications, and credit allocation and extension transactions and approvals, and controls on collateralization, credit limits and lines, credit repayment schedules and calculations, and process of transfer to follow-up accounts, and calculations of allowances and provisions, and classification of credit facilities, and preparation of aging reports, and restructuring transactions, and recognition of transactions, and other controls included in this process; and

c) Accounting and Recognition Process: Interest, income/expense accrual and rediscount calculations; compliance with uniform chart of accounts on transaction basis; depreciation calculations; authorization process relating to issuance of accounting slips; formation of trial balance; existence of authorizations needed for issuance of retrospective accounting slips, and integrity and traceability of records pertaining thereto; assuring sequence and consecutiveness of transaction numbers; control of transaction limits and authorizations; reconciliation between records of branches and head offices; controls on order of chart of accounts and on changes therein; reconciliation between great ledger accounts and subsidiary, sub- and

suspense (provisional) accounts; reconciliation between legal and auxiliary accounting books; and recognition of transactions, and other controls included in this process; and

ç) Alternative Distribution Channels Process: Authorization, identity verification, recognition and other process controls concerning electronic banking / alternative distribution channels; and

d) Debit and Credit Cards Process: Assessment of debit and credit card applications; limit allocation, card printing and distribution transactions; merchant and POS transactions; controls on such applications as use of cards and gift points; process of transfer to follow-up accounts, and calculations of allowances and provisions; preparation of aging reports and restructuring transactions; reconciliation controls such as reconciliation between bank and card centre; and recognition of transactions, and other controls included in this process; and

e) Financial Reporting Process: Control of the process of use of bank records and information sources in financial reporting, and other process controls; and

f) Payment Systems Process: Payment system controls such as EFT (electronic fund transfer), EMKT (electronic securities transfer), Clearing Bank, SWIFT transactions and security records associated therewith, and recognition of transactions, and other controls included in this process; and

g) Treasury / Securities and Fund Management Process: Control of securities and fund management business processes; reconciliations in respect of derivative instruments, nostro, vostro and loro account balances; control of correspondent records, and recognition of transactions, and other controls included in this process.

(3) Efficiency of controls on banking processes is dependent upon efficiency and adequacy of general controls on the related information systems. That is why in the course of inspecting the compatibility, coherence, efficiency and adequacy of controls on banking processes, auditor takes into account the efficiency and adequacy of general controls of information systems as and when deemed fit and necessary. Auditor includes said general controls into the scope of its audit, and evaluates their efficiency and adequacy, as well as their effects on controls on banking processes.

(4) Auditor tests at least the following controls for the processes referred to in second paragraph hereinabove and included in the scope of audit as a result of materiality assessment:

a) Controls affected by management in order to obviate or detect any prevention on effective and efficient operation of controls; and

b) Risk assessment process concerning general controls of information systems and controls of banking processes of auditee; and

c) Controls such as review, reporting, inquiry and reconciliation with regard to supervision of consequences of processes and transactions; and

ç) Controls aimed at supervision of controls; and

d) Controls on accounting and financial reporting process relating to the end of period; and

e) Controls for detection and prevention of such frauds and infractions as repeated information systems and double entry system; and

f) Controls on integrity and reliability of interest, expense, commission, withholding, etc. rates and amounts, maturity and value date information, and data, transactions and records pertaining to other banking information of high concern; and

g) Controls in relation to implementation of the principle of separation of duties; and

ğ) Authorization and access controls, as well as controls regarding review of said controls; and

h) Approval mechanisms included/required to be included in execution of risky transactions; and

ı) Controls on confidentiality of data, transactions and records; and

i) Controls on keeping of audit trails, maintaining of security thereof, and regular review and assessment of them.

Assessment on Internal Control and Internal Audit Systems:

ARTICLE 26 – (1) Auditor assesses within the frame of materiality criterion the works performed by auditee via its internal control and internal audit systems, within the limits of general controls of information systems and controls on banking processes. Accordingly:

a) In the course of inspection of activities conducted in respect of internal control system, at least:

1) Issues in relation with control environment; and
2) Approach adopted by the management for establishment, operation and supervision of an efficient, effective and adequate internal control system, and its implementation; and
3) Application of ethical principles described and outlined in Article 75 of the Law, and level of awareness of employees thereabout

are taken into consideration.

b) Activities performed by internal audit unit for supervision of efficiency, adequacy, compatibility and coherence of internal control system, and performance of internal audit unit are evaluated.

c) As a part of assessment of internal audit unit, the auditee's activities of audit of information systems are also taken into consideration. In the course of assessment of the function of audit of information systems of auditee, at least:

1) Place and independence of team in the organization; and
2) Adequacy of team members in terms of qualifications and number; and
3) Planned and completed audit works; and
4) Follow-up of audit results and consequences

are inspected.

ç) Auditor evaluates and assesses the activities performed in the risk assessment process relating to internal control system of auditee, and its performance therein.

Conduct of Activities of Audit of Information Systems and Banking Processes:

ARTICLE 27 – (1) For performance of BSD activities, independent audit firm must have audit power and must enter into an audit agreement with auditee pursuant to and under this Regulation.

(2) Authorized firms are under obligation to conduct the independent audit activities of auditee as well during the period of conduct of audit on its information systems and banking processes.

(3) Audit of banking processes is conducted by a financial auditor assigned and appointed by the authorized firm for this activity, together with auditor of information systems.

SIXTH PART
Methodology of Audit of Information Systems and Banking Processes

Audit Strategy and Audit Plan:

ARTICLE 28 – (1) For the audit works to be performed, a BSD strategy is created as a basis for development of audit plan and in order to regulate the scope, timing and direction of audit, depending upon the auditor's opinion, in respect of the degree of dependency of auditee's activities to information systems, the degree of complexity of information systems, the economic and financial expectations and their relations with information systems, and adequacy of internal systems of auditee.

(2) BSD strategy contains such issues as scope of audit, materiality assessment to be employed during audit, and material changes that may occur in the audited processes during audit.

(3) Auditor creates and prepares an audit plan compliant with BSD strategy in order to obtain adequate and appropriate audit evidences which may reduce the audit risk to a reasonable level.

(4) In preparation of BSD strategy and plan, internal audit reports, BSD audit reports and correspondences exchanged between auditee and the Agency are taken into consideration.

(5) In the course of BSD planning, a risk assessment work focused on systems and processes of auditee is carried out, and consequences of this work are evaluated and assessed in terms of materiality criterion.

(6) An independent information systems and banking processes audit plan contains at least:

a) Type and timing of audit techniques, and definition of detail level; and

b) Type and timing, and definition of detail level, of risk assessment techniques employed in assessment of material or considerable control deficiency risks; and

c) Planning for reference of audit team and supervision of their activities, by taking into account the individual skills and competences of team members to be assigned for BSD activities.

(7) BSD strategy and audit plan are, if and when deemed necessary in the audit process, documented, updated and amended, together with reasons thereof.

(8) In planning of audit, auditor takes into consideration all risks of error, misconduct and illegal acts.

Audit Techniques and Testing of Controls:

ARTICLE 29 – (1) In order to obtain and collect audit evidences adequate and required for provision of reasonable assurance for formulation of an audit opinion, auditor employs all or some of the following audit techniques with appropriate timing and details:

a) Information collection; and
b) Observation; and
c) Inquiry and verification; and
ç) Re-implementation; and
d) Recalculation; and
e) Analytical examination.

(2) Auditor determines the scope of controls to be tested, by taking the materiality principle into consideration, and in such manner to provide a reasonable assurance to it about efficiency, adequacy, compatibility and coherence of information systems and banking processes of the cluster of

controls to be tested, and of all of the controls applied on these systems and processes.

(3) In order to express an opinion verifying that controls applied on information systems and banking processes are efficient, adequate, compatible and coherent, the efficiency and compatibility of design and operation of all controls inspected thereunder must have been tested.

(4) In order to reduce the audit risk to a reasonable level, auditor details its tests, and expands its sample volume, and increases the adequacy and reliability level of its evidences, in such manner to reduce the detection risk in all areas where the material or considerable control deficiency risk is high in respect of the tested control.

(5) In determining the scope of test regarding control, auditor takes into consideration such control characteristics as the frequency of application of related control, and the period of time trusted for being active, and the expectation of deviation in controls.

(6) Auditor cannot form an opinion on efficiency, adequacy, compatibility and coherence of a control only with audit evidences obtained by using information collection technique.

(7) Auditor determines the time dimension to be taken into consideration while testing a control, in such manner to form an opinion on the whole audit period.

Audit Sampling:

ARTICLE 30 – (1) Audit sampling refers to and stands for application of audit techniques on less than 100 percent of a universe relating to audit so as to assure that all items have the chance to be selected. Audit sampling allows auditor to obtain, collect and assess audit evidences relating to selected samples in such manner to be able to form an opinion about total data set from which samples are taken. In audit sampling, statistical or non-statistical approaches may be used.

(2) In generating the audit sample, auditor is obliged to take into account the purpose of audit technique and the qualities and characteristics of universe from which samples will be selected.

(3) In determining the sample volume, auditor is under obligation to take into account whether audit risk is reduced to an acceptably low level or not.

Sample volume is affected from the audit risk level acceptable to the auditor. As the risk level acceptable to the auditor falls, sample volume must also be increased to the same extent.

(4) Auditor selects samples with the expectation that all sampling units which may be sampled from universe have the chance to be selected. Purpose of sampling is to discover and reveal conclusions relating to the whole universe, and for this reason, auditor endeavours to select samples free of any sort of prejudice and having qualities and characteristics representative of universe.

Audit Evidences:

ARTICLE 31 – (1) Audit evidences mean and cover all information used by auditor with a view to obtaining consequences underlying its opinion as to efficiency, adequacy, compatibility and coherence of controls on information systems and banking processes.

(2) Auditor designs and implements all of the required audit procedures in order to obtain reliable, adequate and appropriate audit evidences underlying its opinion.

(3) The level of required audit evidences regarding efficiency and adequacy of each control selected for testing purposes is dependent upon the probability of the relevant control to cause a material or considerable control deficiency if it does not function or operate.

(4) For the sake of obtaining reliable audit evidences, the information underlying the audit techniques applied by auditor must be complete, true and accurate. Auditor may, in application of its audit techniques, use also any information generated by auditee, providing that it conducts adequate investigation as to completeness and accuracy of said information.

Evaluation of Audit Findings:

ARTICLE 32 – (1) At the end of its audit work, auditor separately inspects each control weakness detected therein, and assesses these weaknesses both individually and in different combinations, and classifies them as considerable control deficiency or material control deficiency by using qualitative and quantitative methods.

(2) In assessing these control weaknesses, auditor mainly takes into consideration the probability of occurrence of mistakes that may be caused by them collectively or separately, and the probable effects of them in case of occurrence.

(3) In assessing the control weaknesses relating to information systems general controls, auditor also takes into consideration the probable effects of them on controls of banking processes.

(4) In case of detection of a control weakness in any one of the following fields during audit works, auditor accepts and considers such weakness at least as considerable control deficiency:

a) Policies concerning implementation of the Turkish Accounting Standards; and
b) Controls needed for enforcement of the Law and the regulations and guidelines issued and published in reliance upon the Law; and
c) Controls or programs for prevention of fraud; and
ç) Non-routine or non-systematic transactions; and
d) Year-end financial reporting process.

(5) In case of detection of any one of the following events, auditor accepts and considers the same at least as considerable control deficiency and perceives each of them as a strong sign or indication of material control deficiency:

a) Corrections required to be made in the already published financial statements due to the assets and liabilities of auditee reflected thereon inaccurately as a result of an error or fraud, to such extent to negatively affect the decisions required to be taken about auditee in terms of legal obligations as defined in the applicable laws, or the conduct of a healthy financial assessment on auditee; and

b) Detection by auditor during audit works of a material misstatement available in the financial statements or data of current period and overlooked by internal control units and departments of auditee; and

c) Detection of an inconsistency between information, documents and data received from different units and departments of auditee about the same issue; and

ç) Detection of a material misstatement in information and statements given by management of auditee to auditor, even if not made maliciously or intentionally; and

d) Failure in performance of commitments given in the action plan; and

e) Where internal audit and risk management functions are considered to be needed for establishment of an effective and efficient internal control environment in the light of profile of auditee, non-existence of aforesaid functions for information systems, or inefficiency of them; and

f) Non-existence of a unit/function in charge of control of compliance with laws within the frame of processes and systems regarding information systems and banking activities, or inefficiency of that unit/function; and

g) Detection of a fraud, even if of small size, involved in by director or directors; and

ğ) Failure in correction of a considerable control deficiency reported to directors within a reasonable period of time; and

h) Failure in establishment of an efficient internal control environment; and

ı) Failure of audit committee to establish an efficient supervision on accounting, financial reporting and internal control system.

Management Statement:

ARTICLE 33 – (1) Bank presents to auditor a management statement issued by its board of directors as of the current audit period about its internal controls on information systems and banking processes.

(2) In forming its audit opinion, the auditor inspects and reviews that management statement and the works underlying that statement. If auditor detects any deficiency or mistake in statement as a result of its inspection, such determinations are also given in its audit report.

(3) If and when auditee's board of directors refuses to give a management statement, then and in this case, individuals authorized to sign BSD report may express a qualified opinion, or refrain from expressing an opinion, or make a proposal to management of authorized firm for withdrawal from audit work within the frame of procedures and principles set down in Article

34 hereof. Thereupon, if authorized firm decides to withdraw, this decision is notified to the Agency, together with reasons thereof, within no later than seven days thereafter.

(4) Procedures and principles relating to management statement and its implementation under this Regulation are determined by the Agency.

Formation of Audit Opinion and Audit Letter:

ARTICLE 34 – (1) If a material control deficiency is not detected as a result of audit, and if a restriction or prevention is not faced during the audit, then, individuals authorized to sign audit report express a positive opinion by using the sample format given in Exhibit-10 hereof, after due consultation with the independent audit teams reporting to them.

(2) Individuals authorized to sign audit report express a qualified opinion by using the sample format given in Exhibit-11 hereof after due consultation with the independent audit teams reporting to them, if and when:

a) they find out at least one material control deficiency as a result of their audit works, but nevertheless, they believe that such control deficiencies do not negatively impact the whole or a large part of information systems and banking processes and systems of auditee; or

b) they cannot obtain or collect adequate information about existence of any problem limiting BSD activities or about a newly established system or process, though not important enough to require them to avoid from expressing an opinion thereon; or

c) they cannot obtain and collect adequate and appropriate audit evidences for formation of an audit opinion.

(3) Individuals authorized to sign audit report express a negative opinion by using the sample format given in Exhibit-12 hereof after due consultation with the independent audit teams reporting to them, if and when they assess and evaluate individually or collectively the material control deficiencies found out as a result of their audit works, and thereupon:

a) they come to a conclusion that such material control deficiencies make negative impacts on the whole or a large part of information systems and banking processes and systems of auditee; or

b) they find out a difference or discrepancy with management statement prepared and issued pursuant to first paragraph of Article 33, which arises out of understatement or wrong statement of a material control deficiency, together with all significant sides, after an audit conducted by auditor in auditee.

(4) In the event that individuals authorized to sign audit report believe and think that uncertainties and limitations confronted during audit works are important enough to preclude them from expressing an opinion, they may, after due consultation with the independent audit teams reporting to them, avoid from expressing an opinion about controls on information systems and banking processes. In this case, audit letter is issued and given by using the sample format given in Exhibit-13 hereof. The report to be issued in case of avoidance from expressing an opinion is required to indicate auditor's opinions on the causes of avoidance.

(5) If, as a result of BSD performed in banks and its partnerships subject to consolidation, positive, qualified or negative opinions are concluded within the frame of the provisions of Articles 5 and 7 of this Regulation and the types of opinions cited in this article, then, an audit letter is issued in accordance with the sample formats given in respectively Exhibit-14, Exhibit-15 and Exhibit-16. In case of circumstances requiring the auditor to avoid from expressing an opinion, audit letter is issued in accordance with the sample format given in Exhibit-17.

Documentation of Audit Works:

ARTICLE 35 – (1) Auditor prepares working papers during the period of audit works with a view to supporting the opinions to be expressed in its report and presenting evidences proving that its audit is planned and conducted in strict compliance with pertinent provisions of this Regulation.

(2) Working papers are prepared in such manner to allow review and assessment of the collected evidences and the audit report before the report is finalized.

(3) Auditor prepares the working papers in such manner to allow a senior experienced auditor not ever involved in the subject audit works to comprehend and understand:

a) compliance of the audit works with pertinent provisions of this Regulation; and

b) consequences of audit evidences collected and of audit techniques applied; and

c) material and major events detected during audit, and assessments finally made in connection therewith.

(4) Working papers may be kept on paper or in electronic media.

(5) Right of discretion on working papers belongs to the authorized firm employing auditor, or if audit is outsourced, to the relevant independent audit firm assigned therefor. Working papers cannot be disclosed or otherwise furnished to third parties outside the Agency without a prior written consent of auditee. It is the responsibility of authorized firm to provide confidentiality and security of working papers.

(6) Authorized firm is under obligation to bring together all working papers within 60 days following the date of audit report. Working papers are kept for a minimum period of five years starting from the date of audit report.

SEVENTH PART
General Principles and Responsibilities

Information Systems and Banking Processes Audit Agreement:

ARTICLE 36 – (1) BSD is conducted within the frame of a written agreement to be signed by and between authorized firm and auditee. BSD agreement indicates the full mutual agreement reached between the parties on scope and contents of audit to be conducted. BSD agreement may be included in the agreement to be entered into pursuant to the Fourth Part of BDYFY.

(2) BSD agreements become effective upon approval by board of directors of auditee.

(3) Except for consolidated BSD agreements, auditee provides the Agency with information about agreement signed by and between auditee and authorized firm, within thirty days following signature of agreement, in accordance with procedures and principles to be determined by the Agency.

(4) Before entering into an audit agreement with auditee, authorized firm is under obligation to conduct the required preliminary investigation so as to determine the scope and planning of BSD. In the course of this preliminary investigation, in the case of existence of incidents which may positively or negatively affect the audit process and in the case of change of authorized

firm, information may be requested about reasons thereof from authorized firms which have performed audit works in the previous periods. Auditee informs the former authorized firm about name of authorized firm contracted for the current period, and authorizes the latter to give and disclose all information requested by the new authorized firm. Thereupon, the former authorized firm is obligated to give and provide all information requested from it accordingly.

(5) BSD agreements are required to contain at least the following items:

a) Regulations which auditor is liable to comply with; and
b) Purpose, scope, and if any, special reasons of BSD; and
c) Services to be offered by authorized firm under the agreement; and
ç) Responsibilities and obligations of the parties thereto; and
d) Auditors to be assigned for audit, and their substitutes; and
e) Job titles of and terms of office stipulated for individuals assigned for the audit team, and detailed breakdown of amounts of fees specified for each of them; and
f) Starting and completion dates of audit process; and
g) Format of audit report and if requested, special purpose audit report, and causes of preparation of these reports; and
ğ) Date of delivery of audit report.

(6) Upon limitation of the field of work of auditor to a material extent in conflict with the terms and conditions of agreement, or failure in collection of information and documents concerning information systems and banking processes, or occurrence of similar other events, the agreement may be terminated by authorized firm, providing that a written justification is filed and a prior notice is sent to the Agency in connection therewith. Authorized firm notifies this termination to the Agency immediately, together with its reasons of withdrawal from audit. Upon withdrawal, authorized firm is liable to permit its successor authorized firm to review and examine all of its working papers and other required information, and if requested, to provide the copies of these documents thereto. Authorized firm appointed in place of the former authorized firm is definitely required to be approved by the Agency.

(7) If auditee carries out some of its activities through a support service provider, then, auditor ensures that its BSD agreement contains terms and conditions allowing it to perform audit works in support service provider as well.

EIGHTH PART
Cooperation in Audit of Information Systems and Banking Processes

Utilization of Works Performed by, and Cooperation with, Other Parties:

ARTICLE 37 – (1) Auditor personally performs adequate works as needed for it to obtain and collect fundamental evidences underlying its opinion. However, with a view to ensuring expansion of its audit works in terms of structure, timing and level of details, auditor may also utilize works of other authorized firms, internal systems units of auditee, and specialized persons and entities.

(2) To utilize works performed by other parties does not reduce liability of auditor in respect of audit. Auditor may not make any reference in its report to the works utilized as above.

(3) Depending on its opinions as to adequacy and independence of internal systems of auditee, in its audit report, auditor takes care of refraining from repetitions as far as possible by taking into consideration the internal audit and internal control activities of auditee.

(4) For the sake of determining at which level of details the works already conducted by other parties may be utilized, senior information systems independent auditor checks and evaluates at least:

a) appropriateness of scope of audit works, and adequacy of audit program; and
b) structure of controls inspected therein; and
c) professional competence, diligence, neutrality and independence of individuals who conduct work works; and
ç) quality of audit works by testing a portion adequate for assessment of the works as a whole.

(5) Authorized firm and auditor performing the previous BSD are obligated to provide new authorized firm and individuals assigned for current BSD with all kinds of information and documents needed for audit within the frame of confidentiality principle.

(6) Internal auditors and individuals in charge of internal control activities in auditee are under obligation to furnish to auditors all information needed by the latter, also including their own reports.

Cooperation Between Agency and Authorized Firms:

ARTICLE 38 – (1) Information disclosed by the Agency in the course of BSD activities performed in auditee may, if required, be shared with the relevant auditors.

(2) The Agency personnel may accompany as observers each stage of BSD process of authorized firms with a view to improving their knowledge and skills, without prejudice to the auditor independence principle. The Agency personnel may not use the know-how of authorized firm for their own personal interests or for interests of another authorized firm. Authorized firm shows great efforts and gives the required contributions for involvement of the Agency personnel in the process and for improvement of their knowledge.

(3) For the sake of enforcement of provisions of second paragraph, authorized firm reports its audit programs in banks to the Agency upon demand of the latter before actual start of its audit works therein.

Audit of Support Service Provider:

ARTICLE 39 – (1) Auditor takes into consideration in which direction and to which extent the services outsourced by auditee influence its information systems and banking processes, and plans its audit works accordingly, and develops an effective audit approach.

(2) Auditor may, as per Article 37 of this Regulation, make use of such documents as audit report and certificate, still current, held by it in respect of services offered by support service provider.

NINTH PART
Information Systems and Banking Processes
Audit Report and Notification

Information Systems and Banking Processes Audit Report:

ARTICLE 40 – (1) BSD report is a text which clearly describes in writing in a plain language the opinion of auditor, and contains assessments on information systems and banking processes, by also taking the materiality concept into consideration. Duty of auditor is to collect, examine and assess audit evidences about controls on information systems and banking processes, and to come to a conclusion on these evidences, thereby forming an opinion about audit.

(2) Auditor is under obligation to issue a BSD report during its audit works. Principles and procedures relating to the report are regulated by the Board.

(3) BSD report covers all of the activities pertaining to the period of audit. Completed reports are signed by senior responsible information systems independent auditor of authorized firm or, if the information systems audit is conducted through outsourcing, by the individual authorized by the related firm to sign the same, and by senior responsible associate auditor defined in BDYFY. If the authorized firm assigns and appoints a senior responsible associate auditor to conduct information systems audit, providing that he meets and satisfies the past experience conditions sought for in this Regulation, then, audit report may be signed by this individual jointly with the other senior responsible associate auditor in lieu of senior responsible information systems auditor.

(4) BSD report is completed together with independent audit report, unless specified otherwise by the Agency, and is submitted to the chair of board of directors and audit committee of auditee, and to the Agency in two copies, in accompaniment of a letter duly signed by individuals authorized to represent and bind authorized firm. An electronic copy of BSD report duly signed by a secure electronic signature formed in accordance with provisions of the Electronic Signature Law no. 5070 dated 15/1/2004 is also sent to the Agency within the same period of time.

(5) Contents of BSD report are classified as confidential information and are not published in any media. Confidentiality and security of these data and information are under responsibility of the Agency, authorized firms, independent audit firms, external service providers and auditee under this Regulation. Auditees are not allowed to give statements reflecting the audit results and cannot use them for advertisement purposes.

TENTH PART
Miscellaneous and Final Provisions

Employment of Auditors in Banks:

ARTICLE 41 – (1) Auditors cannot be employed in or recruited by banks the audit process of which has been participated also by them during the recent two years.

Matters on Which the Regulation Remains Silent:

ARTICLE 42 – (1) All and any matters on which this Regulation remains silent shall be governed by and subject to the procedures and principles set forth in BDYFY, international audit standards and COBIT.

Regulation Repealed:

ARTICLE 43 – (1) The Regulation on Information Systems Audit to be Performed in Banks by Independent Audit Firms, promulgated in the Official Gazette edition 26170 on 16/5/2006 is hereby superseded and repealed.

Transitory Process:

TEMPORARY ARTICLE 1 – (1) Independent audit firms authorized prior to the date of publication of this Regulation are also governed by and subject to the provisions of this Regulation, and auditors, other than assistant auditors, of these firms are under obligation to fill in the statements given in Exhibit-4, Exhibit-5, Exhibit-6 and Exhibit-7 attached hereto and to send the same to the Agency until 31/5/2010.

Exception Clause:

TEMPORARY ARTICLE 2 – (1) Individuals who are actually working as and in the capacity of senior information systems auditor in authorized firms as of the date of promulgation of this Regulation are accepted and deemed to have satisfied the conditions listed in seventh and eighth paragraphs of Article 18 of this Regulation.

Effective Date:

ARTICLE 44 – (1) Article 33 of this Regulation will become effective as of 1/1/2011, and all other provisions hereof will become effective as of the date of promulgation with effect from 31/12/2009.

Enforcement and Execution:

ARTICLE 45 – (1) The provisions of this Regulation will be enforced and executed by the President of Agency.

	Official Gazette edition where this Regulation is published	
	Date	**Edition**
	13/1/2010	27461
	Official Gazette editions where Regulations Amending this Regulation are published	
	Date	**Edition**
1	26/7/2011	28006
2	28/1/2014	28896
3		