COMMUNIQUÉ ON INDEPENDENT AUDIT OF

INFORMATION SYSTEMS

(III-62.2)

(Published in the Official Gazette edition 30292 on 05.01.2018)

List of Amendments:

1. Communiqué (III-62.2.a) Amending Communiqué (III-62.2) on Independent Audit of Information Systems published in the Official Gazette edition 31003 on 09.01.2020

FIRST CHAPTER

Purpose, Scope, Grounds and Definitions

Purpose

ARTICLE 1 – (1) The purpose of this Communiqué is to determine and set down the procedures and principles for independent audit of information systems of Entities, Institutions and Corporations listed in Article 2, and for authorization of independent audit firms to be assigned for such independent audit, and for reporting of results of independent audit.

Scope

ARTICLE 2 – (1) This Communiqué shall be applied in independent audit of information systems of the Entities, Institutions and Corporations listed below:

(a) Borsa İstanbul Inc,

(b) Stock exchanges and market operators and other organized marketplaces,

(c) Private pension funds,

(ç) Istanbul Settlement and Custody Bank Inc.,

(d) Central Securities Depository Inc.,

(e) Portfolio custodians,

(f) Capital Markets Licensing Registry and Training Agency Inc.,

(g) Capital market institutions,

ğ) Publicly held corporations,

(h) Turkish Capital Markets Association,

(ı) Turkish Appraisers Association.

(2) Out of the Entities, Institutions and Corporations listed in the first paragraph, as for the banks and insurance companies pursuant to Article 136 of the Capital Markets Law no. 6362

dated 06.12/.012 and as for the financial leasing, factoring and financing companies pursuant to the Financial Leasing, Factoring and Financing Companies Law no. 6361 dated 21.11.2012, independent audit of information systems within the frame of the principles set forth in their own specific laws and regulations is construed as fulfilment of the obligations stipulated in this Communiqué. The aforesaid Entities, Institutions and Corporations are subject to the provisions of this Communiqué in submission to the Board of independent audit reports of information systems, provided that their own specific laws and regulations are also complied with therein.

(3) Independent audit of information systems shall be performed by independent audit firms duly authorized by the Board for independent audit of information systems in capital markets.

Grounds

ARTICLE 3 – (1) This Communiqué is prepared and issued in reliance upon second paragraph of Article 62 and third paragraph of Article 72 and subparagraphs (c) and (h) of first paragraph of Article 128 of the Law no. 6362.

Definitions and Abbreviations

ARTICLE 4 – (1) In the context of this Communiqué:

(a) "BDS" refers to Turkish Auditing Standards and their annexes and comments put into force by the Public Oversight, Accounting and Auditing Standards Authority;

(b) "Information systems auditor" refers to the auditors assigned by the authorized institution and working under job positions listed in Article 15 hereof;

(c) "BSY Communiqué" refers to the Communiqué on Management of Information Systems, no. VII-128.9 of the Board;

(ç) "Law" refers to the Law no. 6362;

(d) "KGK" refers to the Public Oversight, Accounting and Auditing Standards Authority;

(e) "Control" refers to the full set of policies, procedures, applications and organizational structures established with respect to information systems processes and aiming to build an adequate level of assurance as for achievement of business targets and identification, prevention and correction of undesired events;

(f) "Board" refers to the Capital Markets Board;

(g) "Entities, Institutions and Corporations" refers to the entities, institutions and corporations listed in first paragraph of Article 2;

(ğ) "Communiqué Serial X No. 22" refers to the Communiqué on Independent Audit Standards in Capital Markets, Serial X, No. 22, published in the Official Gazette's repeated edition 26196 on 12.06.2006;

(h) "Capital markets institutions" refers to institutions listed in Article 35 of the Law;

(ı) "Authorized institution" refers to an independent audit firm authorized by the Board to engage in independent audit activities on information systems in the capital markets.

SECOND CHAPTER

General Principles on Independent Audit Activities Related to Information Systems

Purpose and Scope of Independent Audit of Information Systems

ARTICLE 5 – (1) Independent audit of information systems is a process comprised of the stages of forming and reporting of an opinion as a result of assessment, in light of information systems management principles stipulated in the BSY Communiqué, of the information system components such as activities, software and hardware covered by the information systems management and operations, and of the controls established within that system.

(2) Fundamental purpose of independent audit of information systems is to form an opinion on compliance, efficiency and adequacy of information systems of audited Entities, Institutions and Corporations and their internal controls relating to that system in line with the information systems management principles stipulated in BSY Communiqué.

(3) An information systems auditor shall determine the system, activity and control mechanisms to be inspected within information systems from a risk-driven point of view and within the frame of a written plan based on the materiality criterion. Furthermore, information systems auditor makes sure that the scope of audits determined within the frame of materiality criterion is outlined in such manner to provide adequate audit evidences for provision of a reasonable assurance for building an audit opinion as per this Communiqué.

Materiality and Audit Risk

ARTICLE 6 – (1) Materiality is the subject of a consideration based on professional knowledge and experience, and refers to assessment of actual or probable effects or impacts of errors, omissions, breaches of procedures, and unlawful acts which arise or may arise due to weaknesses in controls, on the reporting of financial data and the provision of safe and continuous services by the audited Entities, Institutions and Corporations.

(2) In independent audit of information systems, the materiality concept may be used for planning of audits, and intensification of audit in required areas, and assessment and reporting of findings. Integrity, consistency, reliability, and if and to the extent needed, confidentiality of data and continuity of activities which are sensitive on the part of the auditee, particularly financial data, are the fundamental factors required to be taken into account within the scope of the materiality concept.

(3) In assessment of controls affecting financial reports, elements such as value and frequency of financial transactions conducted by the process or system shall be used, while in assessment of controls not related to financial transactions, elements such as criticality of business processes, cost of systems and operations, size of probable results or consequences of errors, number of transactions/inquiries performed in a certain time interval, nature, description, timing and scope of files kept and reports produced, requirements of service level agreements, and amounts of fines in penal clauses shall be used.

(4) Audit risk refers to the probability of failure of information systems auditor to give a correct opinion due to the following risks:

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

(b) Control risk: Refers to the risk of failure of control in prevention, detection or timely correction of at least one considerable control deficiency due to non-functioning of controls as required or expected.

(c) Detection risk: Refers to the risk of failure of an information systems auditor to detect at least one considerable control deficiency existing in information systems of the audited Entities, Institutions and Corporations.

(5) Significant or considerable control deficiency risk: Refers to the risk of existence of at least one considerable control deficiency in information systems of the audited Entities, Institutions and Corporations. Significant or considerable control deficiency risk arises out of structural risk and control risk.

(6) For reducing the audit risk to a reasonable level, information systems auditor shall employ appropriate audit techniques in such manner to mitigate the detection risk in areas where significant or considerable control deficiency risk is rather high.

Criteria

ARTICLE 7 – (1) Information systems auditor shall employ the following criteria in classification of control deficiencies and weaknesses covered by its detections resulting from its inspections according to the materiality concept:

(**a)** Control weakness: Refers to the failure of the design or operation of a control to allow prevention and detection of errors in a timely manner.

(i) Control deficiency in design refers to non-existence of a control capable of assuring achievement of a control target, or failure of an existing control in achievement of a control target expected from it due to errors in its design, even if it operates and runs exactly as designed.

(ii) Control deficiency in operation refers to non-operation of a properly designed control as designed, or failure of the personnel assigned for control to have the competence and authorization needed for effective and efficient performance of control.

(b) Considerable control deficiency: Refers to a deficiency which cannot be considered insignificant and is caused by existence of a control deficiency or combination of several control deficiencies that may most probably create a negative effect on assuring the integrity, consistency, reliability, and if and to the extent needed, confidentiality of data and continuity of activities of audited Entities, Institutions and Corporations. Deficiencies which may probably create a negative effect on prevention of errors and omissions committed during reliable recording of financial data of the audited Entities, Institutions and Corporations in accordance with the generally accepted accounting standards, and during authorization, processing or reporting of the records are also considered in this category.

(c) Significant control deficiency: Refers to a combination of one or more control weaknesses which may preclude prevention or correction of a significant error in periodical financial reports of audited Entities, Institutions and Corporations, or which may most probably create a significant negative effect on assuring the integrity, consistency, reliability, continuity and if and to the extent needed confidentiality of data related to the activities of the audited Entities, Institutions and Corporations.

Efficiency, Adequacy and Compatibility

ARTICLE 8 – (1) In order for the design of a control to be accepted as efficient, control deficiency in design must not exist in that control, or even if it exists, it should not cause or lead to any significant control deficiency.

(2) In order for the operation of a control to be accepted as efficient, the control deficiency in operation must not exist in that control, or even if it exist, it should not cause or lead to any significant control deficiency.

(3) Adequacy of controls on information systems means that all controls made subject to audit within the frame of the materiality principle have an efficient design, and that these controls are designed so as to generate the consequences expected from them within the frame of their business goals and to eliminate or compensate the risks they may expose to in the course thereof.

(4) Efficiency of controls on information systems means that all controls made subject to audit within the frame of the materiality principle have an efficient and effective operation, and that these controls are designed so as to fulfil the functions and reach the control targets and goals expected from them.

(5) A control may be considered to be compatible only if and when all of the obligations and liabilities mentioned in the Law and in secondary regulations and directives promulgated in reliance upon the Law pertaining to controls are fully met and performed. Compatibility of controls on information systems means that all controls made subject to audit within the frame of the materiality principle are indeed compliant.

Relationship between Independent Audit of Information Systems and Independent Audit

ARTICLE 9 – (1) Independent audit of information systems and independent audit shall be planned and implemented in an interactive approach as they contain components which may affect the scope and consequences of each other.

(2) Information systems auditor, in the course of determining the scope of their independent audit on information systems and performing works and activities in connection therewith, shall take care of not only collecting audit evidence adequate for support of audit opinion, but also supporting the audit risk assessments with respect to independent audit.

(3) If and when an opinion on independent audit of information systems is formulated as "qualified", "adverse" or "disclaimer of an opinion", both the opinion and the findings underlying the opinion shall be communicated in writing to the independent auditor. The liability relating thereto belongs to the board of directors of the relevant Entities, Institutions and Corporations.

(4) Information and documents that may be requested by the independent auditor about information systems and their audit for use in their own independent audit works are required to be submitted to the independent auditor by the information systems auditor.

Assessment on internal control and internal audit system

ARTICLE 10 – (1) The provisions of BDS 315 Standard of Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and its Environment and of BDS 610 Standard of Using the Work of Internal Auditors shall be applicable by analogy on the works performed by the information systems auditor on internal control and internal audit systems of the audited Entities, Institutions and Corporations within the limits of information systems controls within the frame of materiality criterion.

THIRD CHAPTER

Conditions of Eligibility for Independent Audit Activities on Information Systems

Qualifications Sought for in Institutions to be Authorized

ARTICLE 11 – (1) Independent audit firms to be authorized for independent audit of information systems are required:

(a) to be included in the list of firms authorized for independent audit in capital markets;

(b) to employ an adequate number of information systems auditors having sufficient qualifications for performance of independent audit activities on information systems;

(c) to be equipped with adequate technical equipment, documentation and recording systems.

Qualifications Sought for in Information Systems Auditor

ARTICLE 12 – (1) Auditors, other than assistant auditor, to be assigned and appointed for independent audit of information systems are required:

(a) to have and hold an Information Systems Independent Audit License Certificate or a Certificate of Information Systems Auditor (CISA) granted by the Information Systems Audit and Control Association (ISACA);

(b) to have adequate professional knowledge for independent audit of information systems and adequate professional experience as mentioned in Article 15;

(c) not to have been adjudged bankrupt, or convicted of a disgraceful offense or a crime in informatics field;

(ç) not to have been permanently banned from dealing with independent audit or independent information systems audit activities upon being found liable for independent audit activities causing cancellation of authorization of institutions whose independent audit activity license or information systems independent audit activity license is withdrawn pursuant to the capital markets laws or other applicable laws and regulations, or if previously banned from dealing with independent audit activities temporarily for a certain period of time, to have their ban removed by the Board upon the expiration of relevant period;

(d) not to be an officer held liable for activities causing cancellation in institutions one or more of the activity licenses of which are cancelled or stock exchange membership of which is cancelled;

(e) not to have been convicted of any act in breach of the Law or the repealed Capital Markets Law no. 2499;

(f) to be resident in Turkey;

(g) not to have been banned from trading in capital markets within the frame of the applicable laws and regulations; and

(ğ) to be working on full time basis in the relevant independent audit firm.

(2) Assistants of information systems auditors should meet and satisfy the conditions listed in subparagraphs (c), (ç), (d), (e), (f), (g) and (ğ) of first paragraph, and should hold a bachelor's degree.

Application to and Authorization by the Board

ARTICLE 13 – (1) Independent audit firms willing to enter into information systems independent audit activities in capital markets are required to apply to the Board with information and documents containing the following items and contents:

(a) Detailed curriculum vitae of information systems auditors to be assigned for independent audit of information systems also containing their professional past experience, license certificates, trainings received about audit, audit works they were so far involved in, if any, their duties and assignments in those works, and a statement of their residence address, and that they do not have any past criminal records, and have not gone bankrupt, and have not dealt with any trading businesses other than their professional activities, and a copy of each of their diplomas / graduation certificates of their graduate and/or postgraduate studies;

(b) a copy of each of the certificates of training received or given about information systems and information systems independent audit;

(c) a list showing distribution by job positions of audit staff to be assigned for independent audit of information systems;

(ç) written statement wherein the relevant auditor agrees and undertakes to resign from the subject audit services if and when his independence is lost at any time during independent audit of information systems;

(d) information and documents relating to hardware, equipment, documentation and recording system;

(e) in case of a legal relationship or link with another company seated and headquartered abroad, a copy of the contract signed with that other company; and

(f) a statement that a professional liability insurance policy will be taken out for compensation of damages and losses that may arise out of independent audit of information systems.

(2) As a result of onsite inspections to be conducted by the Board for determination of professional and technical competences through examination and assessment of the information and documents listed in first paragraph hereinabove of the independent audit firms which file an application for authorization to perform independent audit of information systems in capital markets, if the Board reaches an opinion that the applicant is adequately competent for performance of subject activities within the relevant fields of business, the Board shall grant to the subject independent audit firm the authorization to perform independent audit of information systems in capital markets.

(3) In the course of assessment of applications, the Board may, if deemed necessary, request additional information and documents. Information and documents detected to be missing or requested in addition by the Board are required to be sent or delivered to the Board within not later than one month following the date of notice received by the institution. If the said period is exceeded, application of the relevant institution shall be cancelled.

(4) Conditions sought for granting an authorization to perform independent audit of information systems under this Communiqué are required to be met and satisfied permanently. Whenever deemed necessary, the Board may check whether or not these conditions are satisfied.

(5) Names of independent audit firms which are authorized to perform independent audit of information systems under this Communiqué shall be announced in the internet website of the Board.

Repeal of Authorization of Independent Audit of Information Systems

ARTICLE 14 – (1) Within the frame of the pertinent provisions of the Law, upon detection of any one of the following breaches, authorization of an authorized firm to perform independent audit of information systems in capital markets may be repealed by the Board:

(a) Loss of any one of the conditions sought for firms to be authorized as stated in Article 11 hereinabove;

(b) Non-compliance with standards, principles and rules relating to acceptance or exchange of duties;

(c) Audit plan and work papers and other information and documents supporting them not found to be adequate for proof of audit works alleged to be performed;

(ç) Actual assignment of auditors in audit works other than those named in the information systems independent audit contract submitted and in the information systems independent audit staff designated and declared to the Board;

(d) Failure to obtain required audit evidences due to failure to employ appropriate audit techniques;

(e) If and when the Board detects that the authorized firm has, in an information systems independent audit assignment, failed to detect some certain failures which may make material and significant negative effects on protection of assets of the audited Entities, Institutions and

Corporations, on conduct of their business activities in accordance with the Law and other applicable laws and regulations, on reliability and integrity of their financial reporting systems, and on timely collection of information, and if the authorized firm fails to demonstrate not to be faulty in said failures;

(f) In an information systems independent audit assignment, failure of the audit team, also including the responsible information systems chief auditor, to comply with such ethical principles as honesty, neutrality, professional competence and diligence, independence, reliability and professional behaviour;

(g) Failure in performance of notification obligations timely, accurately and completely, or in disclosure or provision of any information and documents requested by the Board or by designees of the Board on time, fully, completely and accurately as requested;

(ğ) Issuance of a faulty, incomplete, misleading and untrue information systems independent audit report;

(h) Failure to take out a professional liability insurance policy in such manner to cover also information systems independent audit;

(ı) Not having performed information systems independent audit activities continuously for a period of 5 years.

(2) Upon detection of responsibility in any one of the matters referred to in subparagraph (f) of first paragraph, the Board may forbid permanently or temporarily for a period not being less than 2 years, any information systems independent audit activities in capital markets of only the relevant responsible information systems chief auditor and/or the relevant information systems chief auditor and/or the relevant information systems senior auditor and/or the relevant information systems auditors, depending on the contents of said responsibility. Auditors who are prohibited from performing information systems independent audit activities in capital markets as per this paragraph may, at the end of the period of said ban, apply to the Board for lifting the ban, or otherwise, the ban is applied permanently. Applications to be filed with the Board for lifting the ban at the end of the period of ban by auditors who are prohibited from performing information systems independent audit activities in capital markets temporarily for a certain period of time shall be examined, and concluded by the Board by also taking into account whether or not there is a pending investigation about the applicant. Any applications to be filed with the Board for lifting the ban during the period of ban shall not be taken into consideration.

(3) Before an authorization is repealed permanently or temporarily, defence of the relevant authorized firm and/or information systems auditor shall be taken. Should a defence not be provided within one month following the date of delivery of a summons requesting a defence thereon, the right of defence is deemed to have been waived.

(4) Repeal of information systems independent audit authorization of an authorized firm does not construe as a repeal of its independent audit authorization as well. However, if and when independent audit authorization of an authorized firm is repealed, its information systems

independent audit authorization will also be deemed to have been repealed without any further action.

Job Titles of Auditors

ARTICLE 15 – (1) Information systems auditors shall have the titles; responsible information systems chief auditor, information systems chief auditor, information systems senior auditor, information systems auditor, and information systems assistant auditor according to the order of seniority.

(2) Information systems auditors are required to have graduated from four-years' graduate study programs of universities, or higher education institutions seated abroad equivalency of which are accepted by the relevant official authorities, and to have an actual minimum professional experience of three years, and to hold an Information Systems Independent Audit License Certificate or a Certificate of Information Systems Auditor (CISA) granted by the Information Systems Audit and Control Association (ISACA).

(3) Information systems senior auditors are required to satisfy all of the conditions sought for eligibility for being an information systems auditor, and to have an actual minimum professional experience of 6 years.

(4) Information systems chief auditors are required to satisfy all conditions sought for eligibility for being an information systems auditor, and actually to have a minimum professional experience of 10 years.

(5) Those meeting all conditions set down in the fourth paragraph are, if deemed fit and eligible as a result of assessments made by the Board, assigned as responsible information systems chief auditor. In the assessment to be made by the Board, a resolution of board of directors containing a statement that the relevant responsible information systems chief auditor is authorized and liable to sign the audit reports in the name of its company, is required to be submitted.

(6) A responsible information systems chief auditor is a natural person who has the title of an information systems chief auditor in an independent audit firm, and conducts the information systems independent audit works under his own responsibility in the name of the firm, and is authorized to sign the audit reports in the name of the firm.

(7) Total sum of periods of time spent in any one or more of information systems independent audit, professional information systems control or security, and information systems development and operation activities is considered and treated as professional experience under this Communiqué.

(8) In evaluation of professional experience conditions, a Certificate of Information Systems Auditor (CISA), a Certificate of Internal Auditor (CIA), or a post-graduate degree received in disciplines pertaining to information systems is considered and treated as an additional 1 year of information systems independent audit experience, while a doctorate degree received in disciplines pertaining to information systems is considered and treated as additional 2 years of information systems independent audit experience.

(9) Promotions to any job titles, other than the responsible information systems chief auditor title, shall be effected by relevant authorities. Those who do not meet the qualifications sought for the upper level in terms of knowledge, skills and competence may not be promoted to the upper level, even if they satisfy the professional experience condition.

(10) All staff of authorized firms appointed for information systems independent audit under this Communiqué are under obligation to receive or provide continuous training in the field of independent audit of information systems for at least 20 hours each year and at least 80 hours in 3 years.

Distribution of Duties, Powers and Responsibilities in Team Work

ARTICLE 16 – (1) For each audit, an audit team comprised of two members, at least one of them being a permanent member and the other being a reserve member, shall be appointed, and each audit work shall be performed by a team composed of auditors of a number and of qualifications needed for the specific work, being at least one member. In teams comprised of an information systems chief auditor, an information systems senior auditor or an information systems auditor under chair of a responsible information systems chief auditor, the duties, powers and responsibilities shall be distributed according to the following criteria:

(a) The responsible information systems chief auditor is obligated to decide on compliance of information systems to BSY Communiqué, in addition to the duties, powers and responsibilities of auditors.

(b) Information systems chief auditor and information systems senior auditor share the duties and responsibilities of auditors on such issues as planning and conduct of audit activities, examination of work papers, performance of required revisions, and negotiations with officers of the audited Entities, Institutions and Corporations, and refer to the responsible information systems chief auditor for final decision on material issues.

(c) Information systems auditor shall be in charge of detailed audit works such as preparation of an audit program. Information systems auditor shall be liable and authorized on items of works such as allocation of assistant auditors for works, supervision of their works, examination of their work papers, personal performance of more complex and difficult parts of audit works, making required changes in the work program, and management of negotiations with the audited Entities, Institutions and Corporations during the audit works.

Ethical Principles to be Complied with by Authorized Firms and Auditors

ARTICLE 17 – (1) The Ethical Rules for Independent Auditors published by the KGK shall be applied by analogy as the ethical principles to be complied with by authorized firms and information systems auditors.

FOURTH CHAPTER

Obligations and Audit Methodology Relating to Information Systems Independent Audit Activities

Obligations of Audited Entities, Institutions and Corporations

ARTICLE 18 – (1) Audited Entities, Institutions and Corporations are under obligation to make information systems documentation and all kinds of records, information, documents, structures and systems regarding such documentation ready and fit for audit works.

(2) Audited Entities, Institutions and Corporations are obligated to provide all kinds of information and documents that may be requested by an information systems auditor for independent audit of information systems.

(3) Entities, Institutions and Corporations submit to the information systems auditor a copy of the internal audit reports, if any, upon the request of the latter, and take required actions and measures as needed for establishment of cooperation between the information systems auditor and the internal auditors of the audited Entities, Institutions and Corporations. They further ensure that internal auditors respond to and clarify the questions asked by the auditors of the authorized firm in a timely manner.

(4) It is the responsibility of the board of directors of audited Entities, Institutions and Corporations to inform the board of directors of audited Entities, Institutions and Corporations about findings of information systems auditors, and to ensure coordination among auditors, directors, and personnel of audited Entities, Institutions and Corporations.

(5) Audited Entities, Institutions and Corporations are obligated to present to the information systems auditor a management statement approved by the board of directors providing assurance about internal controls relating to information systems as of the audit period. Management statement shall be prepared in such manner to cover the contents listed in Annex 1 to this Communiqué.

(6) Audited Entities, Institutions and Corporations shall decide and implement by an action plan their commitments regarding resolution of the findings set down in the audit report. It is under the responsibility of the board of directors of audited Entities, Institutions and Corporations to ensure that the action plan is implemented and the commitments given in the action plan are fulfilled timely and completely.

(7) Provisions of special laws and regulations pertaining to the field of business of audited Entities, Institutions and Corporations are, however, reserved.

Obligations of Authorized Firms and Auditors

ARTICLE 19 – (1) Information systems auditors are under obligation to comply with professional guidelines and ethical principles required by their profession, and to prepare an audit plan by taking into account the risks and weaknesses that may be contained in information systems and within the frame of professional scepticism, and to present this action plan to the

auditee and implement the same, and not to accept and treat the statements of managers as an adequate audit proof, and to create the audit report.

(2) Quality assurance system required to be established by independent audit firms pursuant to the provisions of the Communiqué, Serial X, No. 22, shall be carried out in such manner to cover also information systems independent audit works performed by authorized firms, and information systems independent audit reports resulting therefrom.

(3) Information systems auditor is under obligation to provide managers of the auditee and the audit committee of the audited Entities, Institutions and Corporations with information about errors and abuses detected in its audit in writing at each stage of audit works.

(4) Any changes in documents and statements mentioned in Article 13 are required to be reported to the Board within six business days. Changes in audit staff shall also be reported to the Board, together with reasons thereof.

(5) Authorized firms are under obligation to ensure that the information systems auditors they employed attend the related training programs continuously.

(6) During information systems independent audit activities, if and when any transactions in breach of the underlying laws and regulations or any incidents which may lead to expression of an adverse opinion or disclaimer of opinion are detected, even if the audited Entities, Institutions and Corporations have already resolved or eliminated them, such transactions or incidents are required to be reported in writing by the information systems auditor to the Board within ten business days following the date of their detection. In cases that constitute a crime pursuant to the Law and other applicable laws and regulations, such incidents shall also be reported to the relevant official authorities urgently, and further notified to the Board in writing.

(7) Information systems auditor shall immediately inform the audited Entities, Institutions and Corporations or their managers in writing or verbally about all and any incidents or matters found important, including, but not limited to, the ones listed below, which may be detected during information systems independent audit:

(a) Overall approach and scope of information systems independent audit, including probable restrictions and additional works;

(b) Disruptions relating to policy formulation process, problems in policy applications, or changes in policy applications which make or may make a significant impact on information systems;

(c) Uncertainties that may arouse doubt on continuity of activities of the audited Entities, Institutions and Corporations;

(ç) Disagreements with managers of audited Entities, Institutions and Corporations on issues which may have material effects on information systems or audit report;

(d) Material weaknesses and risks contained in information systems.

(8) Where information is provided verbally, information systems independent auditor includes in the work papers both the incidents reported as above and the answers received.

(9) Information systems auditors are under obligation to keep all documentation and documents provided to them by related persons in the course of information systems independent audit works in good faith and unchanged till the end of the period they are needed for their audit works and to return them at the end of their audit works. Copies of the documents constituting audit evidence may be kept by the authorized firm.

(10) Authorized firms and information systems auditors shall take measures to protect data and information which come to their attention in the course of their information systems independent audit activities and that are classified as confidential under relevant legislation, and not to disclose such data and information to third parties other than those who are clearly authorized by laws, and not to use the same directly or indirectly in their own interests or in interests of third parties.

(11) In case of failure of audited Entities, Institutions and Corporations to disclose or furnish to information systems auditors any information and documents relating to information systems independent audit, this failure shall be urgently reported by the authorized firm to the Board.

(12) The authorized firm is under obligation to take out a professional liability insurance with a coverage also including risks that may arise out of audit of information systems.

(13) The authorized firm is obligated to send to the Board upon request all of the work papers and all kinds of audit-related information and documents that may be issued or provided by information systems auditors it employs, or to present the same to Board staff authorized for inspection.

(14) Authorized firms are liable to prepare implementation directives approved by the board of directors for provisions of Communiqué, Serial X, No. 22, or BDS that are applicable by analogy. The Board is authorized to direct implementation in relation to provisions applicable by analogy.

(15) Information systems auditors may not take office or serve as chairperson or member of board of directors, general manager, manager or vice manager or in other positions having significant decision making powers or responsibilities in audited Entities, Institutions and Corporations the information systems independent audit process of which they have actually participated during the recent two years.

Information Systems Independent Audit Contract

ARTICLE 20 – (1) The Entities, Institutions and Corporations sign the information systems independent audit contract with authorized firm hired for information systems independent audit works within the initial 4 months of the period to be audited. BDS 210 Standards of Agreeing the Terms of Audit Engagements are applicable by analogy on information systems independent audit contract as well.

(2) If an information systems independent audit contract cannot be signed for any reason whatsoever, this event shall be reported to the Board in no later than the first business day following the date of occurrence thereof.

(3) In determination of maximum period of information systems independent audit services to be provided by an authorized firm to Entities, Institutions and Corporations, provisions of second paragraph of Article 400 of the Turkish Commercial Code no. 6102 dated 13.01.2011 shall be applied.

(4) Authorized firms are under obligation to send to the Board the signed information systems independent audit contracts within maximum 6 business days.

(5) Authorized firm and the Entities, Institutions and Corporations are not entitled to come to mutual agreement to terminate an information systems independent audit contract. However, in case of reasonable grounds verified by the Board, the Entities, Institutions and Corporations and the authorized firms may terminate an information systems independent audit contract with prior permission of the Board by providing written justification.

(6) In case of termination, the authorized firm is under obligation to deliver to the Board its work papers and notes and all other required data and information for transfer to its successor authorized firm.

Audit Plan

ARTICLE 21 – (1) The provisions of BDS 300 Standards of Planning an Audit of Financial Statements are applicable by analogy on planning of independent audit of information systems.

Audit Evidence, Techniques, Sampling and Control Test

ARTICLE 22 – (1) The provisions of BDS 500 Audit Evidence Standard, BDS 520 Analytical Procedures Standard and BDS 530 Audit Sampling Standard are applicable by analogy on audit evidence, techniques and sampling as well.

(2) Information systems auditor shall determine the scope of to-be-tested controls by taking into account the materiality principle and in such manner to obtain a reasonable assurance about efficiency, adequacy and compatibility of information systems of the cluster of controls to be tested and of all controls applied on this system.

(3) In order to express an opinion verifying efficiency, adequacy and compatibility of information systems controls, the efficiency and compatibility of design and operation of all controls subject to examination must have been tested.

(4) In order to reduce the audit risk to a reasonable level, information systems auditor shall detail its tests, expand its sampling volume, and increase the adequacy and reliability levels of its evidences in such manner to mitigate detection risk in areas where material or considerable control deficiency risks are high in respect of the controls tested.

(5) In determining the scope of tests related to controls, information systems auditor shall take into consideration such control characteristics as frequency of application of the related control, period trusted in terms of being active, and expectation of deviation in controls.

(6) Information systems auditor shall not form an opinion on efficiency, adequacy and compatibility of a control with only audit evidences obtained by using the information collection technique.

(7) Information systems auditor shall determine the time dimension to be taken into consideration in testing a control in such manner to form an opinion on the whole audit period.

FIFTH CHAPTER

Principles on Reporting of Results of Information Systems Independent Audit

Findings

ARTICLE 23 – (1) Information systems auditor shall report considerable and material control deficiencies by classifying and supporting with adequate and appropriate audit evidences.

(2) In reporting findings, information systems auditor shall provide information about criteria and status of these findings to the extent required for audit purposes.

(3) Findings described as control weakness shall be reported in writing by information systems auditor to managers of the audited Entities, Institutions and Corporations. Information systems auditor shall include in its report both a statement of reporting these findings to managers of the audited Entities, Institutions and Corporations, and the number of control weaknesses detected for each control target.

(4) Information systems auditor shall evaluate in its report all control deficiencies and weaknesses detected in past periods and stated in previous period's audit report to be still outstanding. Its report shall contain statements as to the last status of these control deficiencies and weaknesses, whether or not they are ongoing, and their compliance with the action plan committed by audited Entities, Institutions and Corporations.

(5) Information systems auditor shall code the findings detected in its audits according to the method described in Annex 2 to this Communiqué.

(6) If information systems auditor comes to the conclusion of existence of any one or more of such incidents as abuse, unlawful practices, breach of contract, misconduct, double recording system or duplicated information systems in reliance upon audit evidences collected, all such incidents are required to be included in their its report. These incidents shall be separately reported urgently in writing to the Board by the responsible information systems chief auditor.

Opinions of Audited Entities, Institutions and Corporations

ARTICLE 24 – (1) Information systems auditor shall also provide in their report the opinions of audited Entities, Institutions and Corporations about deficiencies detected, and corrective actions planned to be taken in relation therewith, if any, and probable consequences of such actions.

(2) Information systems auditor shall also include in their report the opinions of audited Entities, Institutions and Corporations with regard to control deficiencies and weaknesses detected in past periods and stated in the previous period's report to be still outstanding, as well as the works performed by the auditee for removal of said weaknesses and deficiencies.

(3) Where the audited Entities, Institutions and Corporations cannot express an opinion or refuse to express an opinion, information systems auditor shall report this event as well, together with reasons thereof.

Conclusive Assessment on Findings

ARTICLE 25 – (1) Information systems auditor shall interpret the audit purposes, audit findings, and if any, opinions of the audited Entities, Institutions and Corporations, and shall provide in their report comments and assessments in line with their own deductions and opinions. Information systems auditor shall makes interpret in its report how the findings resulting from audit works should be understood.

(2) If information systems auditor disagrees with opinions of audited Entities, Institutions and Corporations or considers that the planned corrective actions and works are not appropriate, they shall separately make a reference thereto in their conclusive assessment. If information systems auditor agrees with opinions of the audited Entities, Institutions and Corporations, the required corrections shall be made in the report accordingly.

(3) In the event that a statement as to correction of any control weakness or deficiency is transmitted or reported by audited Entities, Institutions and Corporations to information systems auditor at any time prior to the date of report, for only once for each of the findings, information systems auditor shall analyse and check the final status with regard to the relevant finding in order to verify the statement of the auditee, and if information systems auditor reaches the opinion that the subject control weakness or deficiency is in fact remedied, then they shall report such correction in the conclusive final assessment section of the report pertaining to that finding.

(4) In the conclusive assessment section of the report relating to findings and determinations as to control weaknesses and deficiencies detected in the past periods and stated in the previous period's report to be still outstanding, information systems auditor shall refer to both the compliance of the auditee with the action plan for resolution of the problem, and the recent status of the subject weakness or deficiency as follows:

(a) continuing,

(b) partially corrected,

(c) corrected.

Information Systems Independent Audit Report

ARTICLE 26 – (1) Information systems independent audit report contains opinions of information systems auditor about the audited information systems.

(2) The audit opinion shall clearly state whether the information systems and all of the controls on this system are efficient, adequate and compliant, or not. Information systems auditor shall formulate their opinion thereon within the frame of BSY Communiqué.

Formulation of Information Systems Independent Audit Opinion

ARTICLE 27 – (1) Persons authorized to sign the information systems independent audit report shall express an unqualified opinion in accordance with the sample format provided in Annex 3 to this Communiqué if no material control deficiency is detected as a result of audit, and no restriction or prevention is encountered during the audit.

(2) Persons authorized to sign the information systems independent audit report shall express a qualified opinion in accordance with the sample format provided in Annex 4 to this Communiqué if:

(a) they detect at least one material control deficiency as a result of their audit works, but nevertheless think that such deficiency does not affect the whole or a substantial part of information systems of the audited Entities, Institutions and Corporations;

(b) there exists any incident which restricts the audit activities or they cannot acquire adequate information about a newly established system, though both not being significant enough to require them to issue disclaimer of an opinion;

(c) they fail to collect adequate and appropriate audit evidence for the formulation of an audit opinion.

(3) Persons authorized to sign the information systems independent audit report shall express an adverse opinion in accordance with the sample format provided in Annex 5 to this Communiqué upon assessment of the material control deficiencies detected as a result of their audit works individually or collectively if:

(a) they are of the opinion that such deficiencies affect the whole or a substantial part of information systems of the audited Entities, Institutions and Corporations;

(b) they detect a discrepancy from the management statement arising out of deficient or incorrect reporting in all material aspects of a material control deficiency as a result of an audit performed by information systems auditor in audited Entities, Institutions and Corporations.

(4) Persons authorized to sign the information systems independent audit report may issue disclaimer of an opinion if and when they believe that uncertainties and limitations confronted in audit works are material enough to prevent expression of an opinion thereon. In this case, they shall issue disclaimer of an opinion in accordance with the sample format provided in Annex 6 of this Communiqué. Report to be issued in case of disclaimer of an opinion is required to explain the auditor opinions on causes leading to this outcome.

(5) BDS 705 Modifications to the Opinion in the Independent Auditor's Report is applicable by analogy for expression of qualified or adverse opinion in information systems independent audit report or for issuing disclaimer of an opinion.

Basic Elements of Information Systems Independent Audit Reports

ARTICLE 28 – (1) Report to be issued by information systems auditor shall contain the following basic elements:

(a) Heading,

(b) Authority to whom the report is presented,

(c) Introductory paragraph,

(ç) Information on audit works,

(d) General information about information systems of the audited Entities, Institutions and Corporations,

(e) General assessment on internal control and internal audit structure relating to information systems of the audited Entities, Institutions and Corporations,

(f) Auditor opinion,

(g) Abbreviations and terminology, and

(ğ) List of annexes and footnotes.

Finalization and Notification to the Board of Information Systems Independent Audit Report

ARTICLE 29 – (1) Information systems independent audit report of Entities, Institutions and Corporations becomes final when signed by the relevant responsible information systems chief auditor. Information systems independent audit report shall be delivered to the chair of board of directors of the audited Entities, Institutions and Corporations until the close of business in the first business day following the date it is finalized. Information systems report received by the board of directors of the audited Entities, Institutions and Corporations shall then be sent to the Board, together with a resolution of the board of directors as to acceptance of report, within no later than 5 business days thereafter.

(2) Information systems independent audit report shall be completed and sent to the Board within 30 days following the end of the relevant audit period. If the last day of delivery of information systems reports coincides with an official holiday, the first business day following the official holiday is accepted and treated as the last day of notification.

SIXTH CHAPTER

Obligations, Exemptions, Effective Date and Enforcement

Obligations and Exemptions

ARTICLE 30 – (1) Borsa İstanbul Inc., Istanbul Settlement and Custody Bank Inc., Central Registry Agency Inc., stock exchanges and market operators and other organized marketplaces, central clearing institutions, central custodians and trade repositories are under obligation to have an information systems independent audit conducted once a year pursuant to this Communiqué. These Entities, Institutions and Corporations are required to have their first information systems independent audit conducted for the year in which this Communiqué entered into force, and have their subsequent information systems independent audit conducted for the year following the previous one.

(2) Partially and broadly authorized intermediary institutions and portfolio management companies the minimum shareholders' equity requirement of which is more than 5 million TL, are under obligation to have an information systems independent audit conducted once every 2 years pursuant to this Communiqué. These Entities, Institutions and Corporations are required to have their first information systems independent audit conducted for the second year following the year in which this Communiqué entered into force, and have their subsequent information systems independent audit conducted for the second year following the previous one.

(3) Portfolio management companies the minimum shareholders' equity requirement of which is equal to or less than 5 million TL, and Capital Markets Licensing Registry and Training Agency Inc. are under obligation to have an information systems independent audit conducted once every three years pursuant to this Communiqué. These Entities, Institutions and Corporations are required to have their first information systems independent audit conducted for the third year following the year in which this Communiqué entered into force, and have their subsequent information systems independent audit conducted for the third year following the previous one.

(4) Narrowly authorized intermediary institutions, publicly held corporations, collective investment firms, asset leasing companies, private pension funds, house financing funds, asset financing funds, mortgage financing institutions, independent audit, rating and appraisal firms, Turkish Capital Markets Association, Turkish Appraisers Association and other capital market organizations, the establishment and operating principles of which are determined by the Board, are not under obligation to have an information systems independent audit conducted pursuant to this Communiqué.

(5) The Board is authorized to remove any or all of the obligations and exemptions set down in first, second, third and fourth paragraphs of this Article, and to change the scope and contents thereof separately for the Entities, Institutions and Corporations.

(6) **(Added: OG 09.01.2020 – 31003)** With respect to the minimum shareholders equity requirement under the second and third paragraphs, the amounts determined and announced by the Board in relation to revaluation under Articles 28 and 41 of Communiqué (III-55.1) on Principles Regarding Portfolio Management Companies and Activities of Such Companies published in Official Gazette edition 28695 on 02.07.2013, shall be basis.

Matters on Which This Communiqué Remains Silent

ARTICLE 31 – (1) All and any matters on which this Communiqué remains silent shall be governed by the procedures and principles set down in BDS and best professional practices.

Transitory Provisions

TRANSITIONAL ARTICLE 1 – (1) Independent audit firms authorized by the Banking Regulation and Supervision Agency on audit of information systems and banking processes of banks may be temporarily authorized to perform independent audit of information systems of the Entities, Institutions and Corporations for a term of one year without having the authorization to conduct information systems independent audit in capital markets, providing

that they apply to the Board within 60 days following the effective date of this Communiqué. Said independent audit firms are thereafter required to be specifically authorized by the Board for the subsequent years under this Communiqué.

(2) The limitation of 4 months imposed by Article 20 hereof on signature of information systems independent audit contract is not applicable for the first audit period.

Effective Date

ARTICLE 32 – (1) This Communiqué will become effective as of the date of its publication.

Enforcement

ARTICLE 33 – (1) The provisions of this Communiqué are enforced and executed by the Capital Markets Board.

ANNEX-1

Principles on Management Statement

1) Purpose

The purpose of management statement is to provide assurance as to existing situation and the works performed in relation therewith through the assessment made by the board of directors of Entities, Institutions and Corporations on efficiency, adequacy and compatibility of their internal controls on information systems for the relevant information systems independent audit period.

2) Scope

Entities, Institutions and Corporations shall take into consideration the scope of information systems independent audit described in Article 5 of this Communiqué in the process of forming an opinion in the framework of management statement as to efficiency, adequacy and compatibility of the internal controls on information systems.

Areas to be assessed within information systems shall be identified from a risk-driven point of view and based on the materiality criterion. The scope of this assessment shall be determined in such manner to collect adequate audit evidence to be able to provide reasonable assurance for an opinion to be expressed on the whole information systems in management statement.

Management statement shall be issued only in relation to the internal controls on information systems. In formulating a management statement, the support services received shall also be taken into consideration.

3) Period

The board of directors of Entities, Institutions and Corporations shall formulate the management statement as a result of works and assessments performed on the current information systems audit period. The period to be used is 1 January – 31 December, and as of the end of this period, the board of directors shall make a statement in conformity with the date of information systems independent audit report.

4) Contents

Management statement shall declares as a minimum the following points with clear and definite wording:

a) That Entities, Institutions and Corporations are under obligation to establish and operate an efficient, adequate and compatible internal control system with respect to Communiqué VII-128.9 on Management of Information Systems,;

b) That the relevant units have already examined the internal control system and made an assessment in order to put forth all material control deficiencies about that system;

c) That it is declared that the works conducted by independent audit firm are not used in the assessment made by the relevant units about the internal control system as cited above;

ç) The material control deficiencies, if any, detected on the internal control system;

d) That the internal control system does not have any material control deficiency, other than those clearly declared, which may prevent the efficiency, adequacy and compatibility of the system in the light of the procedures and principles set down in Article 10 of this Communiqué and in the Communiqué VII-128.9 on Management of Information Systems,;

e) That all control weaknesses and all considerable and material control deficiencies relating to the internal control system detected in the course of the assessments made on internal control system – even if later corrected as of the end of period – have been classified and presented to the information systems independent auditor;

f) All abuse or corruption that cause a material misstatement in financial statements, or materially affect the integrity, consistency, reliability, and if and to the extent required, confidentiality of data, especially financial data, which are sensitive on the part of Entities, Institutions and Corporations, or materially affect the continuity or sustainability of their activities, or even if not at a material level, are involved in by managers or other officers having critical job duties in the internal control system;

g) That the existing situation as to whether or not the findings that have already been detected in previous information systems independent audits and presented to the relevant Entities, Institutions and Corporations, but are not yet approved by the authorized institution to have been resolved, are resolved, is already described in the attachment to the management statement;

h) Changes which have occurred in the internal control system or in other items that may materially affect the internal control system, at any time after the examinations conducted on the internal control system, in such manner to cover also the corrective actions taken by the Entities, Institutions and Corporations with respect to material and remarkable control deficiencies.

ANNEX-2

Coding of Findings Detected in

Information Systems Audits

Findings detected by independent audit firms in information systems audits shall be coded as described below.

Audit Year	•	K/S	•	Control Area	•	Finding Sequence No.	•	Materiality Degree	•	Materiality Degree 2

Explanations of fields used in coding are as follows:

Audit Year: In this field, the audit year when the finding is detected shall be inserted in four digits (2016, 2017 …).

K/S: Letter "K" is used for consolidated information systems audit findings, while letter "S" is used for solo information systems audit findings.

Control Area: In this field, abbreviation of control area where the finding is detected shall be entered.

Control Areas	Abbreviations
Management of Information Systems	**BSY**
Construction and implementation of information systems management	BSY-1
Information security policy	BSY-2
Supervision and responsibility of senior management	BSY-3
Information systems risk management	BSY-4
Security test	BSY-5
Others	BSY-DGR
Principles on Information Systems Controls	**BSK**
Establishment and management of information systems controls	BSK-1
Asset management	BSK-2
Separation of duties principle	BSK-3
Physical and environmental security	BSK-4
Network security	BSK-5
Identity verification	BSK-6
Authorization	BSK-7
Integrity of transactions, records and data	BSK-8
Data confidentiality	BSK-9
Management of services outsourced with respect to information systems	BSK-10
Confidentiality of customer data and information	BSK-11
Information of customers	BSK-12
Exchange of information with third parties	BSK-13

Creation of audit trails	BSK-14
Time Synchronization	BSK-15
Information Security Breach	BSK-16
Acquisition, development and maintenance of information systems	BSK-17
Continuity of information systems	BSK-18
Change management	BSK-19
Others	BSK-DGR

Finding Sequence No.: In this area, all findings included in the solo information systems audit report are numbered starting from **1 for every year,** independently from the process and audit areas they are detected. The findings in the consolidated information systems audit report are also numbered starting from **1 for every year,** independently from the corporation, process and audit areas they are detected. After this number, the finding's sequence number shall be entered in three digits (such as 001, 162, etc.).

Materiality Degree: In this area, the materiality degree assigned to the finding upon first detection shall be entered. This data shall not be changed in subsequent periods. "KZ" abbreviation shall be used for findings classified as a control weakness, "KD" abbreviation shall be used for findings classified as a remarkable control deficiency, and "ÖK" abbreviation shall be used for findings classified as a material control deficiency.

Materiality Degree 2: If a materiality degree of a finding detected in the previous period changes as of the current period, this area shall be used for inserting the new materiality degree of that finding. If materiality degree of a finding is changed for more than once, materiality degree given to that finding as of the last situation is inserted in this area. **This area shall be left blank if there is no change in materiality degree of the finding.**

Sample Codings:

2016.S.BSY-1.003.ÖK.KD

2014.S.BSK-2.152.ÖK

2015.K.BSY-3.045.KD

ANNEX-3

INFORMATION SYSTEMS INDEPENDENT AUDIT OPINION

(Unqualified Opinion)

TO: …….. Inc. Board of Directors

We have been assigned to audit the information systems of …….. Inc. as of …/…./…. pursuant to and under Communiqué III-62.2 on Independent Audit of Information Systems.

[Explanations on Responsibility of Board of Directors of Entities, Institutions and Corporations:]

It is under the responsibility of Management of ……. Inc. to ensure that information systems controls are established in the auditee, and are efficiently operated, and an adequate control system is built therein, in accordance with the procedures and principles set forth in Communiqué VII-128.9 on Management of Information Systems.

[Explanations on Responsibility of Authorized Audit Firm:]

We, as the firm assigned for independent audit of information systems, are responsible for expressing an opinion in reliance upon our audit work. Our audit work has been planned so as to provide reasonable assurance for detection of material control deficiencies existing in the information systems of the auditee, and has been conducted in accordance with the principles and procedures set down in Communiqué III-62.2 on Independent Audit of Information Systems. Audit covers the testing and assessment of design and operation efficiency and compatibility of information systems controls within the frame of materiality principle, and the implementation of similar other audit techniques to the extent needed.

We believe that the audit conducted has created a reasonable and adequate ground for forming of our opinion.

[Natural Limitations]

Due to restrictions inherent to controls, there may be information systems control deficiencies which may be undetected. In addition, the results obtained in reliance on our findings should not be evaluated so as to cover future periods. These results are exposed to the risk of changing by time due to such reasons as change in existing conditions, changes made in systems or controls, or distortion of the degree of efficiency of controls.

[Auditor Opinion]

In our opinion, efficient, adequate and compatible controls have been established on the information systems of …….. Inc. as of …/…./…. in all material aspects thereof in accordance with the principles and procedures set down in Communiqué VII-128.9 on Management of Information Systems.

Date and Place of Issue

Name and Surname & Signature of

Responsible Information Systems

Chief Auditor

Trade Name of Institution

ANNEX-4

INFORMATION SYSTEMS INDEPENDENT AUDIT OPINION

(Qualified Opinion)

TO: …….. Inc. Board of Directors

We have been assigned to audit the information systems of …….. Inc. as of …/…./…. pursuant to and under the Communiqué III-62.2 on Independent Audit of Information Systems..

[Explanations on Responsibility of Board of Directors of Entities, Institutions and Corporations:]

It is under the responsibility of Management of ……. Inc. to ensure that information systems controls are established in the auditee, and are efficiently operated, and an adequate control system is built therein, in accordance with the procedures and principles set forth in Communiqué VII-128.9 on Management of Information Systems.

[Explanations on Responsibility of Authorized Audit Firm:]

We, as the firm assigned for independent audit of information systems, are responsible for expressing an opinion in reliance on our audit work. Our audit work has been planned so as to provide a reasonable assurance for detection of material control deficiencies existing in the information systems of the auditee, and has been conducted in accordance with the principles and procedures set down in Communiqué III-62.2 on Independent Audit of Information Systems.. Audit covers the testing and assessment of design and operation efficiency and compatibility of information systems controls within the frame of materiality principle, and the implementation of similar other audit techniques to the extent needed.

We believe that the audit conducted by us has created a reasonable and adequate ground for forming of our opinion.

[Natural Limitations]

Due to restrictions inherent to controls, there may be information systems control deficiencies which may be undetected. In addition, the results obtained in reliance on our findings should not be evaluated so as to cover future periods. These results are exposed to the risk of changing by time due to such reasons as change in existing conditions, changes made in systems or controls, or distortion of the degree of efficiency of controls.

[Reasons and grounds of auditor opinion as to limitations put on audit activities and as to processes, practices and controls which cannot be audited for that reason; and material control deficiencies detected with respect to information systems of the auditee, and as to why these control deficiencies do not affect the whole or a great part of the information systems of the auditee]

In our opinion, due to the reason(s) referred to above (in paragraph …), except for the probable effects of these reason(s) on the information systems of the auditee, efficient, adequate and compatible controls have been established on the information systems of …….. Inc. as of …/…./…. in all material aspects thereof in accordance with the principles and procedures set down in the Communiqué on Management of Information Systems, no. VII-128.9.

Date and Place of Issue

Name and Surname & Signature of

Responsible Information Systems

Chief Auditor

Trade Name of Institution

ANNEX-5

INFORMATION SYSTEMS INDEPENDENT AUDIT OPINION

(Adverse Opinion)

TO: …….. Inc. Board of Directors

We have been assigned to audit the information systems of …….. Inc. as of …/…./…. pursuant to and under Communiqué III-62.2 on Independent Audit of Information Systems.

[Explanations on Responsibility of Board of Directors of Entities, Institutions and Corporations:]

It is under the responsibility of Management of ……. Inc. to make sure that information systems controls are established in the auditee, and are efficiently operated, and an adequate control system is built therein, in accordance with the procedures and principles set forth in Communiqué VII-128.9 on Management of Information Systems.

[Explanations on Responsibility of Authorized Audit Firm:]

We, as the firm assigned for independent audit of information systems, are responsible for expressing an opinion in reliance on our audit work. Our audit work has been planned so as to provide a reasonable assurance for detection of material control deficiencies existing in the information systems of the auditee, and has been conducted in accordance with the principles and procedures set down in Communiqué III-62.2 on Independent Audit of Information Systems.. Audit covers the testing and assessment of design and operation efficiency and compatibility of information systems controls within the frame of materiality principle, and the implementation of similar other audit techniques to the extent needed.

We believe that the audit conducted by us has created a reasonable and adequate ground for forming of our opinion.

[Natural Limitations]

Due to inherent restrictions inherent to the nature of controls, there may be information systems control deficiencies which may be undetected. In addition, the results obtained in reliance upon our findings should not be evaluated so as to cover future periods. These results are exposed to the risk of changing by time due to such reasons as change in existing conditions, changes made in systems or controls, or distortion of the degree of efficiency of controls.

[Reasons indicating why the information systems controls of the auditee are not found efficient, adequate and compatible]

[Auditor Opinion]

In our opinion, due to the reason(s) explained above (in paragraph …), efficient, adequate and compatible controls have not been established on the information systems of ……..

Inc. as of …/…./…. in all material aspects thereof in accordance with the principles and procedures set down in Communiqué VII-128.9 on Management of Information Systems, no..

Date and Place of Issue

Name and Surname & Signature of

Responsible Information Systems

Chief Auditor

Trade Name of Institution

ANNEX-6

INFORMATION SYSTEMS INDEPENDENT AUDIT OPINION

(Disclaimer of an Opinion)

TO: …….. Inc. Board of Directors

We have been assigned to audit the information systems of …….. Inc. as of …/…./…. pursuant to and under Communiqué III-62.2 on Independent Audit of Information Systems.

[Explanations on Responsibility of Board of Directors of Entities, Institutions and Corporations:]

It is under the responsibility of Management of ……. Inc. to make sure that information systems controls are established in the auditee, and are efficiently operated, and an adequate control system is built therein, in accordance with the procedures and principles set forth in Communiqué VII-128.9 on Management of Information Systems.

[Explanations on Responsibility of Authorized Audit Firm:]

We, as the firm assigned for independent audit of information systems, are responsible for expressing an opinion in reliance on our audit work. Our audit work has been planned so as to provide a reasonable assurance for detection of material control deficiencies existing in the information systems of the auditee, and has been conducted in accordance with the principles and procedures set down in Communiqué III-62.2 on Independent Audit of Information Systems. Audit covers the testing and assessment of design and operation efficiency and compatibility of information systems controls within the frame of materiality principle, and the implementation of similar other audit techniques to the extent needed.

[Reasons of issuing disclaimer of an opinion by the auditor]

[Auditor Opinion]

Due to the reason(s) explained above (in paragraph …), we are issuing disclaimer of an opinion on efficiency, adequacy and compatibility of controls established on the information systems of …….. Inc. as of …/…./….

Date and Place of Issue

Name and Surname & Signature of
Responsible Information Systems
Chief Auditor

Trade Name of Institution