COMMUNIQUÉ ON MANAGEMENT OF INFORMATION SYSTEMS (VII-128.9)

(Published in the Official Gazette edition 30292 on 5/1/2018)

List of Amendments:

1. Communiqué (VII-128.9.a) Amending Communiqué (VII-128.9) on Management 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 management of information systems of Entities, Institutions and Corporations listed in Article 2.

Scope

ARTICLE 2 – (1) The Entities, Institutions and Corporations listed below are under obligation to comply with the provisions of this Communiqué:

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,

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, and

ı) Turkish Association of Appraisal Experts.

(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 6/12/2012 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, management of information systems within the frame of the principles set forth in their own specific laws and regulations is construed as performance of the obligations stipulated in this Communiqué.

Grounds

ARTICLE 3 – (1) This Communiqué is prepared and issued in reliance upon subparagraph (h) of first paragraph of Article 128 of the Law no. 6362.

Definitions and Abbreviations

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

(a) "Primary systems" refers to the whole system comprised of infrastructures, hardware, software and data ensuring registration and use of the information needed by the Entities, Institutions and Corporations for performance of their duties and obligations arising out of the Law and the associated regulations and statutory instruments safely and in such manner to make sure that they are available at all times on-demand in electronic media;

(b) "Integrity" refers to the feature of protection of accuracy and completeness of information;

(c) "Audit trail" refers to records ensuring step-by-step follow-up of financial or operational transactions and information security breaches from the beginning to the end, as well as records indicating the transactions on those records;

(ç) "Corrective action" refers to actions taking after any emergency, error, failure or abuse incident in information systems with a view to diminishing the effects of such incident;

(d) "Availability" refers to the feature of accessibility and usability of information whenever requested by authorized user, application or system;

(e) "Confidentiality" refers to availability of information systems and information only to authorized user, application or system;

(f) "Safe area" refers to an area hosting information processing, communication and storage hardware and equipment;

(g) "Secondary systems" refers to primary system backups ensuring that in case of an interruption in activities conducted through primary systems, these activities are made sustainable within a recovery time objective as specified in the business continuity plan, and that all information is available continuously and whenever requested as and when needed for performance of obligations and liabilities identified for Entities, Institutions and Corporations in the Law, and associated regulations;

(ğ) "Law" refers to and stands for the Law no. 6362;

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

(ı) "Board" refers to and stands for the Capital Markets Board;

(i) "Entities, Institutions and Corporations" refers to the entities, institutions and corporations listed in Article 2;

(j) "Policy" refers to a document indicating the principles and objectives of Entities, Institutions and Corporations and approved by their top management;

(k) "Procedure" refers to a document defining transactions and actions regarding processes;

(l) "Capital market institutions" refers to institutions listed in Article 35 of the Law;

(m) "Process" refers to continuous transactions and actions forming the modus operandi of performance and production of a work;

(n) "Third Party" refers to natural persons or legal entities other than Entities, Institutions and Corporations and customers;

(o) "Senior management" refers to an individual or a group identified by the board of directors, or if no identification is made by the board of directors, the highest echelon officer of relevant Entities, Institutions and Corporations.

SECOND CHAPTER

Management of Information Systems

Establishment and Implementation of Management of Information Systems

ARTICLE 5 – (1) Management of information systems shall be treated as a part of corporate governance practices. In order for Entities, Institutions and Corporations to be able to perform and continue their operations in a stable, competitive, developing and safe line, the compliance of their strategies relating to information systems with their business goals and objectives shall be ensured, and elements with regard to management of information systems shall be included in managerial hierarchy, and the financing and human resources required for correct management of information systems shall be allocated for the sake of their security, performance, effectiveness, accuracy and sustainability.

(2) Entities, Institutions and Corporations establish policies, processes and procedures relating to management of information systems, regularly review the same, and ensure that they are kept current in line with changes in business fields or technological advancements and are then communicated to all relevant organization units.

Information Security Policy

ARTICLE 6 – (1) An information security policy covering establishment, operation, management and use of information systems and aiming to protect confidentiality and integrity

of information and to ensure that all information is available whenever requested or needed shall be prepared by senior management and approved by board of directors. The approved information security policy shall be communicated to the staff. This policy shall cover definition of roles and responsibilities required for operation of information security processes, and formation of processes as to management of risks related to information systems, and establishment and supervision of controls in relation therewith.

Supervision and Responsibility of Senior Management

ARTICLE 7 – (1) Implementation of information security policy shall be supervised by senior management. It is the responsibility of board of directors to establish effective and adequate controls on information system as a requirement of information security policy.

(2) Critical projects relating to commissioning of new information systems shall be reviewed by senior management, and approved by considering the manageability of risks pertaining to them. Regardless of whether critical projects are carried out by means of internal resources of Entities, Institutions and Corporations or by means of outsourced services, personnel specialization is required to be capable of meeting technical requirements of projects. Managerial roles and responsibilities to be formed in order to support this structure shall also be determined clearly.

(3) Senior management of Entities, Institutions and Corporations shall show determination in taking information security measures at an appropriate level, and shall allocate adequate resources for the activities to be carried out for that purpose. Senior management shall establish at a minimum the mechanisms required for performance of the following activities and operations:

a) Review and approval of information security policies and all liabilities and responsibilities pertaining thereto every year;

b) Determination of potential risks relating to information systems and processes, together with effects thereof, and within this framework, performance of risk management containing definition of activities aimed at diminishing and reducing said risks;

c) Monitoring of incidents relating to information security breaches, and annual assessment of these incidents;

ç) Performance of activities and provision of trainings aimed at increasing information security awareness of all employees.

(4) Processes and procedures established for management of risks relating to information systems shall be incorporated into organizational and managerial structures of Entities, Institutions and Corporations in an actually operable manner, and their operability shall then be supervised and monitored.

(5) An information systems security supervisor who is responsible for fulfilling and monitoring the requirements of processes and procedures relating to security of information systems, reports to senior management about risks pertaining to security of information systems

and about management of those risks, and has adequate technical knowledge and experiences in connection therewith shall be assigned.

(6) According to risk priorities, a business continuity plan shall be prepared in order to ensure sustainability of all critical business processes. This plan shall cover recovery time objective and recovery point objective regarding critical business processes.

Information Systems Risk Management

ARTICLE 8 – (1) Entities, Institutions and Corporations shall establish and keep current certain risk management processes and procedures in order to measure, monitor, process and report the risks regarding information systems.

(2) At least, the following factors shall be taken into consideration in management of risks relating to information systems:

a) Negative consequences of failure to keep pace with developments in competitive environment due to quick developments in information technologies, and difficulties in keeping pace with developments, and probable changes or amendments in applicable laws and regulations;

b) The possibility that use of information systems may pave the way for unforeseeable errors and fraudulent transactions;

c) The risk of dependence to outsourcing service providers due to use of outsources in information systems;

ç) Businesses and services becoming substantially dependent on information systems;

d) It becoming difficult to assure security of transactions carried out via information systems and of data and records kept regarding audit trails.

(3) A risk analysis shall be performed on information systems. It shall then be repeated at least once a year or upon occurrence of material changes in information systems.

(4) Information shall be collected in a timely manner about technical vulnerabilities in information systems, weakness of the institution against such types of vulnerabilities shall be assessed, and appropriate measures shall be taken for handling of the resulting risks.

(5) Information systems of Entities, Institutions and Corporations shall be subject to a penetration test at least once a year by natural persons or legal entities holding a national or international certificate on penetration testing and not having any duties regarding fulfilment of requirements of information security.

(6) In penetration tests, the principles and procedures described in Annex 1 to this Communiqué shall be applied.

THIRD CHAPTER

Principles on Information Systems Controls

Establishment and Management of Information Systems Controls

ARTICLE 9 – (1) As a requirement of information security policy, in order to make sure that security risks arising out of information systems are managed at an adequate level, senior management of Entities, Institutions and Corporations shall ensure that controls are developed, operated, run and kept current with respect to measures aimed at confidentiality, integrity and availability of information systems and of data held therein for processing, transmission and storage purposes, and shall define the required managerial responsibilities in connection therewith.

(2) At least, the following factors shall be taken into consideration in terms of information systems controls:

a) Clear definition of process owner, roles, activities and responsibilities for each control process;

b) Periodical definition of control processes;

c) Clear definition of objectives and purposes of each control process, and measurability of its performance.

(3) Effectiveness, adequacy and appropriateness of information systems controls, and activities aimed at reducing the effects of foreseen risk or risks shall be continuously monitored, and assessed. Material control deficiencies detected as a result of assessment shall be reported to senior management so as to ensure that the required measures are taken.

Asset Management

ARTICLE 10 – (1) Entities, Institutions and Corporations shall determine the information assets they own and the supervisors responsible for those assets, and keep an inventory of the assets, and keep this inventory current.

(2) Information assets shall be classified according to their degrees of significance.

(3) Portable media shall be protected against loss or theft risks depending on the degree of sensitivity of information contained therein, and portable media hosting information with a high degree of significance or software providing access to such information are not allowed to be removed out of the institution without prior authorization.

(4) Before storage media are disposed of, necessary measures and actions shall be taken in order to ensure that they do not contain any data, information and licensed software belonging to the institution.

(5) Clear desk and clear screen principles shall be adopted and applied.

Segregation of Duties Principle

ARTICLE 11 – (1) Areas of duties and responsibilities shall be separated in order to reduce error, deficiency or abuse risks on information systems. The segregation of duties principle shall be applied in systems, databases and applications that are in development, testing and production phases. Duties and responsibilities shall be reviewed in certain time intervals so as to be kept current at all times.

(2) In designing the information systems processes, non-dependence of critical operations to a single personnel or a single outsourcing service provider shall be taken into consideration.

(3) Where it is not possible to separate duties fully and appropriately, compensatory controls shall be established in order to prevent and detect errors, deficiencies and abuses.

Physical and Environmental Security

ARTICLE 12 – (1) Safe areas shall be protected by required entrance controls with a view to making sure that physical access is open only to authorized persons.

(2) Entries to and exits from safe areas shall be reasoned, authorized, recorded and monitored.

(3) Physical protections shall be designed and applied against damages caused by fire, flood, earthquake, explosion, pillage and other natural or manmade disasters.

Network Security

ARTICLE 13 - (1) Controls shall be built and effectively managed for protection of networks against threats and for the sake of security of systems, databases and applications using networks.

(2) Communication infrastructures shall be protected against eavesdropping and physical damages.

(3) Security measures shall be taken and implemented for risks related to access of mobile devices to the network.

(4) Unauthorized accesses to the infrastructure of information systems shall be prevented, and supervision processes shall be built and established.

(5) Restrictions on connection time shall be used in order to enhance and upgrade the security level of highly risky applications.

(6) Security criteria, service levels and management requirements of all kinds of network services procured from internal sources or acquired through outsourcing shall be defined, and included in the service agreements pertaining thereto.

(7) Authorizations shall be made as required to control users having remote access. To this end, automatic equipment identification shall be taken into consideration in order to authorize connections coming from certain locations and equipment.

(8) In communications with networks other than the corporate network, for threats that may come from external networks, firewall solutions kept continuously under supervision shall be employed.

(9) Sub-sections of internal network having different security requirements shall be separated from each other, and controls used for controlled access shall be built.

Authentication

ARTICLE 14 – (1) For transactions executed through information systems, an authentication method fit to the results of risk assessment shall be determined. In choice of method, kind of transactions planned to be executed through information systems, size of their probable financial or non-financial effects, sensitivity of subject data, and ease of use of the chosen authentication method shall be taken into consideration.

(2) Authentication method shall be applied in such manner to cover the whole process from inclusion of customers and staff into information systems to the time they complete their transactions and leave the system. Measures shall be taken as required to guarantee accuracy of authentication information from the beginning to the end of the session. In authentication methods requiring use of password, passwords shall be ensured to be of a complexity and length difficult to be predicted and broken.

(3) Measures and actions required for ensuring security of media where authentication data are kept and of tools used for that purpose shall be duly taken. These measures shall include at least encrypted storage of authentication data, establishment of systems capable of perceiving all kinds of change or modification in said data, keeping of adequate audit trails, and ensuring their security. Actions shall also be taken for the sake of confidentiality of authentication data during transfer thereof.

Authorization

ARTICLE 15 – (1) Entities, Institutions and Corporations shall establish an appropriate authorization and access control for access to information systems. In appointment of authorization level and access rights, by taking into consideration relevant duties and responsibilities, an approach of appointment of the principle of least privilege and of grant of the most restricted right of access shall be adopted. The authority and responsibilities to be appointed shall be kept consistent with the segregation of duties principle.

(2) All authorities and rights of access are subject to reassessment every year in terms to their compliance with the then-current situation.

(3) Authorization data shall be kept in security, and systems shall be established for perception of all kinds of changes in these data. Unauthorized access attempts to media used for keeping the authorization data shall be recorded, and regularly reviewed.

(4) In case of termination of employment, all relevant authorizations shall be urgently cancelled.

Integrity of Transactions, Records and Data

ARTICLE 16 – (1) Entities, Institutions and Corporations shall take required measures and actions for the sake of integrity of transactions, records and data kept in information systems. Measures aimed at ensuring integrity shall be taken and built in such manner to cover all data transmission, processing and storage stages. The same approach shall also be adopted for the transactions executed in the outsourcing service providers with regard to information systems.

(2) Techniques capable of detecting probable distortions in critical transactions, records and data shall be employed.

Data Confidentiality

ARTICLE 17 – (1) Entities, Institutions and Corporations shall take measures required to assure confidentiality of transactions executed within the frame of information systems activities and of data transmitted, processed and stored as a part of these transactions. Actions to be taken to assure confidentiality will at least include the following steps:

a) Taking required actions and measures fit to the degree of significance of data by taking into consideration the structure of information systems and the variety of acts and transactions;

b) Determination of the rights of access to data within the frame of duties and responsibilities of individuals, and keeping records of accesses, and protection of these records against unauthorized accesses and interventions;

c) If encryption techniques are used to assure data confidentiality, use of only algorithms with proven reliability and robustness, prevention of use of encryption keys invalidated, stolen or broken, and determination of the frequency of change or renewal of encryption keys depending on the level of significance of data and operations.

(2) Entities, Institutions and Partnerships shall take required measures to prevent malicious or inadvertent leakage out of the institution of data of a high degree of significance transmitted, processed and stored with respect to transactions executed within the frame of the information systems activities.

Management of Outsourced Services Relating to Information Systems

ARTICLE 18 – (1) Senior management of Entities, Institutions and Corporations shall establish a supervision mechanism that allows assessment and management at an adequate level of probable risks of services to be outsourced within the frame of information systems, and effective management of relations with firms providing the outsourced services. The supervision mechanism established as above shall contain as a minimum the following elements:

a) Conformity of all systems and processes employed with respect to the information systems services received through outsourcing with the own principles of Entities, Institutions and Corporations regarding their risk management, security, confidentiality and customer confidentiality;

b) Where it is required to transfer data belonging to Entities, Institutions and Corporations to the firm providing information systems services through outsourcing, the principles and practices of said firm in relation to information security should at least be at the same level with that of the Entities, Institutions and Corporations;

c) All and any issues relating to information systems services received through outsourcing should be arranged by keeping in mind the business continuity of Entities, Institutions and Corporations, and all required measures should be taken;

ç) Entities, Institutions and Corporations should be held finally liable and responsible for measurement, assessment, reporting and security functions in information systems services received through outsourcing;

d) Services received through outsourcing should not prevent the performance by Entities, Institutions and Corporations of their legal duties and obligations, and their effective supervision;

e) Before entering into a contract with the outsourcing service provider with respect to material issues, Entities, Institutions and Corporations should conduct an inspection and assessment in the relevant service provider in such manner to cover also whether the service provider has the required technical equipment and infrastructure, financial strength, experience, know-how and human resources adequate for provision of outsourced services at the desired quality level, and should present to senior management their technical competency report to be issued as a result of such inspection and assessment.

(2) Terms and conditions, scope and all kinds of other definitions and provisions regarding use of outsourcing are required to be documented in a contract which is to be signed also by the firm providing the outsourced services. The contract, will include as a minimum the following elements:

a) Definitions regarding service levels;

b) Terms and conditions regarding termination of services;

c) Sanctions to be applied if and when the service is unexpectedly terminated or interrupted;

ç) Requirements relating to material issues within the frame of information security policies of Entities, Institutions and Corporations;

d) In case of a product to be produced under the contract, provisions setting down details including ownership and intellectual and industrial property rights of the product;

e) Clauses aiming to ensure that the contract provisions describing the duties and obligations of the firm providing the services received through outsourcing are also incorporated as binding articles in the contracts to be entered into with subcontractors in connection therewith;

f) Obligation of service provider to disclose and provide in the desired format and at the requested time, all kinds of information that may be requested by the Board pursuant to capital market legislation, and right of the Board to access to all kinds of information,

documents and records kept at the service provider as and when deemed fit and necessary with respect to the services provided under the contract.

(3) Rights of access granted to firms providing services received through outsourcing shall be specifically evaluated. For these accesses, either physical or logical, a risk assessment shall be performed, and if needed, additional controls shall be established. In the course of risk assessment, type of access needed, significance of data to be accessed and effects of access on information security shall be taken into consideration. If and when services are terminated, all rights of access relating thereto shall be cancelled.

(4) Senior management of Entities, Institutions and Corporations shall appoint supervisors having adequate knowledge and experience in order to closely monitor the availability, performance and quality of services received through outsourcing, and the security breach incidents that occur in relation with such services, and security controls, financial conditions and compliance with contract of the firm providing outsourced services.

Confidentiality of Customer Data

ARTICLE 19 - (1) Entities, Institutions and Corporations shall establish control and take all measures as required for the sake of ensuring confidentiality of customer information acquired or stored through information systems.

(2) Entities, Institutions and Corporations shall take all measures required for ensuring that their staff act in conformity with the objectives of protection and processing of personal data. All and any matters on which this Article remains silent shall be governed by the pertinent provisions of the Personal Data Protection Law no. 6698 dated 24/3/2016.

Notification of Customers

ARTICLE 20 – (1) Customers to whom services are provided in electronic media by Entities, Institutions and Corporations shall be clearly informed about terms and conditions, risks and exceptional situations relating to services, and accordingly, information security principles adopted for diminishing the effects of risks of subject services, and methods required to be employed so as to be protected against those risks shall be presented to the attention of the customers.

(2) Mechanisms through which probable problems of customers arising out of information systems and out of services provided in reliance upon information systems can be followed up, and which allow customers to report their complaints shall be established. Then, complaints and warnings shall be assessed, and actions shall be taken for troubleshooting purposes.

Exchange of Information with Third Parties:

ARTICLE 21 – (1) Required security requirements shall be defined and applied before providing third parties with the right of access to information systems of Entities, Institutions and Corporations. Information containing media of Entities, Institutions and Corporations shall be protected against probable abuse or corruption during exchange of information with third parties.

(2) Measures to be taken by Entities, Institutions and Corporations pursuant to the first paragraph may not prevent actions of the Board for collection of information.

Establishment of a Recording Mechanism

ARTICLE 22 – (1) Entities, Institutions and Corporations shall establish an effective audit trail recording mechanism regarding use of information systems by taking into consideration the risks on information systems, and the complexity and width of scope of the systems or activities pertaining thereto. Thus, audit trails of the acts or transactions performed within information systems and causing modifications or deletions in records regarding activities of Entities, Institutions and Corporations shall be ensured to be recorded in adequate detail and clarity. Precautions shall be taken for protection of the recording mechanism against unauthorized systemic and user accesses.

(2) Techniques required for prevention of corruption of integrity of audit trails and for detection of all distortions, if any, shall be employed. Integrity of audit trails shall be regularly reviewed, and extraordinary situations shall be reported to senior management.

(3) Audit trails shall contain at least the following information:

a) Type and description of transactions executed;

b) Unauthorized access attempts relating to transactions;

c) Application executing the transaction;

ç) Identity of person executing the transaction;

d) Timing of transactions.

(4) Audit trails shall be stored for a minimum period of 5 years. Audit trails shall be stored in media having an adequate security level, and shall be backed up, and by doing so, they shall be made available for a foreseen period also after the probable negative incidents in connection therewith.

(5) Outsourcing service providers, customers and staff shall be informed that records are kept about all activities performed on information systems.

(6) Keeping of audit trails does not change or prejudice the obligations of the Entities, Institutions and Corporations relating to keeping of documents as per other provisions of applicable laws and regulations.

Time Synchronization

ARTICLE 23 – (1) Timing data used in information systems by Entities, Institutions and Corporations shall be synchronized according to a single reference source. Timing data shall be acquired by means of atomic clocks.

Breach of Information Security

ARTICLE 24 – (1) Entities, Institutions and Corporations shall establish controls required for management of all kinds of incidents of breach of information security in their own organization

and of resulting weaknesses regarding information systems. These controls shall contain at least the following steps:

a) Establishing mechanisms, determining responsibilities, and informing of all staff, as and when required for recording and solution of breaches committed or the resulting weaknesses as soon as possible;

b) Informing the person reporting the incident of breach or weakness about the consequences of steps taken;

c) Finding the root cause of all incidents of breach and all resulting weaknesses reported as above, and implementation of corrective actions in connection therewith;

ç) Reporting of critical incidents of breach or weaknesses to senior management;

d) Recording of types, time of occurrence, information systems affected by and business processes and impact area of all breaches and weaknesses, of corrective actions performed against then, and time, cost and workforce spent in relation therewith;

e) Ensuring the preparedness of the organization for repeated or similar other breaches or weaknesses.

Acquisition, Development and Maintenance of Information Systems

ARTICLE 25 – (1) Entities, Institutions and Corporations shall establish controls required for acquisition, development and maintenance of information systems. These controls shall contain at least the following elements:

a) For all kinds of information systems, that will be developed or modified in-house by Entities, Institutions and Corporations or to be acquired through outsourcing, the functional requirements together with technical and security requirements for each of the design, development and test phases shall be documented in writing.

b) Structure of the information systems to be acquired is required to be compatible with the scale of the relevant Entities, Institutions and Corporations, the nature and complexity of their activities and the products they offer;

c) In order to monitor and follow up the development of work during information systems development, modification or acquisition activities, project development and progress reports shall be prepared, and approved by the board of directors of relevant Entities, Institutions and Corporations;

ç) Planning, testing and implementation steps regarding updates or modifications shall be handled in detail so as to ensure that material and significant updates or modifications to be made in information systems do not interrupt or preclude business processes and do not constitute an information security risk;

d) Appropriate controls shall be established so as to ensure that data entries in applications are done completely, correctly and validly, that all transactions made on data produce

correct results, and that data and transaction losses, and unauthorized modification or abuse of data are prevented;

e) In determining application security and availability requirements, data classification and risk priorities determined by the organization shall be taken into account;

f) Before information systems are commissioned for use in production environment, their acceptance criteria shall be determined, and they shall be subject to functional, technical and security requirements tests according to a plan to be prepared, and test data shall be carefully selected, protected and controlled;

g) If and when needed, a modified or newly developed system, before being commissioned for use in production environment, shall continue to be operated together with the old system until reaching a certain maturity level; and where such parallel operation is not possible, until the modified or newly developed system reaches a certain maturity level, the old system shall be kept ready for commissioning without any loss of data;

ğ) Training materials required with respect to use of information systems shall be prepared;

h) Transactions executed in development, testing and production environments, and environments where these transactions are executed shall be separated from each other against unauthorized access and modification risks.

Continuity of Information Systems

ARTICLE 26 – (1) Entities, Institutions and Corporations are obligated to keep their primary and secondary systems domestically.

(2) Entities, Institutions and Corporations shall prepare an information systems continuity plan, being a part of the business continuity plan, for the sake of continuity of information systems supporting their activities and operations.

(3) A secondary system shall be established under the plan, or agreements assuring the procurement of this service from support service providers shall be signed. In the secondary system, data and system backups of Entities, Institutions and Corporations shall be kept ready for use.

(4) The plan shall be prepared for information systems services supporting the critical business processes, by also taking into consideration the objectives set down in the business continuity plan. Within this framework, alternative recovery processes and procedures ensuring reopening of services for use shall be established, and the required measures and actions shall be taken.

(5) Under the plan, performance shall be followed up, capacity planning shall be made, and use of system resources shall be monitored.

(6) Necessary measures shall be taken against interruptions that may be caused by infrastructure of information systems, and against incidents that may reduce the transaction performance or suspend the business continuity.

(7) Risk assessment, risk reduction and risk monitoring activities shall be carried out for the sake of continuity of information systems.

(8) The plan shall be reviewed and updated after the changes that may affect the business processes or information systems. Tests shall be conducted to ensure effectivity and currency of plan, outsourcing service providers, if any, shall also be included in the tests, and test results shall be reported to top management. Tests shall be repeated every year.

(9) Information systems shall be backed up in accordance with priorities in the business continuity plan, and processes required for restoring from backup shall be incorporated into information systems continuity plan and test.

(10) Entities, Institutions and Corporations shall keep current versions of the information security policy, information systems continuity plan, network topology, information systems asset inventory and other documents that are material for business continuity and security and passwords regarding management of information systems in safe environments

Change Management

ARTICLE 27 – (1) Entities, Institutions and Corporations shall develop controls for the purpose of management of changes made in all kinds of software, hardware and infrastructure components, documentation and information constituting the information systems. These controls shall contain at least the following contents:

a) For all kinds of changes to be made therein, records describing the reason, scope, impact, risks, and expected benefits of changes, persons assigned for changes, cost thereof, as well as the required test and training activities shall be kept and created;

b) The planned changes shall not be processed unless and until they undergo an approval process;

c) Arrangements relating to planned changes, commissioning dates, test and training activities shall be communicated to all relevant parties in advance;

ç) Return procedures to be applied in case of errors or unforeseeable circumstances in the course of implementation of changes, and responsibilities in connection therewith shall be predetermined;

d) Results of changes made shall be reviewed;

e) All changes realized, cancelled or rejected shall be recorded, documented and kept, together with reasons thereof.

FOURTH CHAPTER

Exemptions, Other Provisions,

Effective Date and Enforcement

Exemptions

ARTICLE 28 – (1) Portfolio management companies, the minimum shareholders' equity liability of which is equal to or less than 5 million TL, and Capital Markets Licensing Registry and Training Agency Inc. are not obliged to implement Articles 24 and 27.

(2) Narrowly authorized intermediary institutions, asset leasing companies, mortgage financing institutions, Capital Markets Association of Turkey, Association of Appraisal Experts of Turkey, independent audit, rating and appraisal firms, publicly held corporations, asset finance funds, collective investment schemes, private pension funds and houseing financing funds are not obliged to implement the provisions of fifth paragraph of Article 7, fourth, fifth and sixth paragraphs of Article 8, third paragraph of Article 14, third paragraph of Article 15, second paragraph of Article 17, fourth paragraph of Article 18, second paragraph of Article 22, Article 24, subparagraphs (b), (d) and (ğ) of first paragraph of Article 25, third paragraph of Article 26 and Article 27.

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

(4) (Added: OG 09.01.2020 – 31003) With respect to the minimum shareholders equity requirement under the first paragraph, 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.

Other Provisions

ARTICLE 29 – (1) On the basis of the provisions of this Communiqué, the principles and rules set down in the relevant Board regulations with respect to data processing infrastructures of intermediary institutions dealing with trading of over-the-counter derivative instruments are applicable.

Effective Date

ARTICLE 30 – (1) This Communiqué will become effective as of the date its publication.

Enforcement

ARTICLE 31 – (1) The provisions of this Communiqué shall be enforced and executed by the Board.

ANNEX-1

Procedures and Principles of

Information Systems Penetration Tests

(1) Purpose: Purpose of penetration tests is to proactively detect, prevent and correct the attempts of penetration into systems by using vulnerabilities and weaknesses detected in information systems of Entities, Institutions and Corporations.

(2) Scope: Tests to be performed as a part of penetration tests cover at least the following headings:

a) Communication Infrastructure and Active Devices,

b) DNS Services,

c) Domain Area and User Computers,

ç) E-mail Services,

d) Database Systems,

e) Web Applications,

f) Mobile Applications,

g) Wireless Network Systems,

ğ) Distributed Denial of Service Tests, and

h) Social Engineering Tests.

(3) Methodology: Penetration tests are comprised of tests to be performed via access points defined by user profiles detailed below. Tests start with system detection, service detection and vulnerability scanning/research steps, and continue with steps to be taken and implemented at each access point. Vulnerabilities and findings detected as a result of these tests shall be examined and reported in detail under each heading related thereto and listed in the section 'Scope' above. During performance of penetration tests, vulnerabilities and findings detected under each test heading shall be assessed and evaluated not only individually, but also in terms of risks and vulnerabilities they may cause when combined, and thereafter, new vulnerabilities and findings detected as a result of this assessment in combination shall also be reported. The findings shall be presented in accordance with the format defined in the **"Finding Format"** section by using the degrees listed in the **"Finding Significance Degrees"** section. Accordingly, while determining the finding significance degrees, the value of asset shall not be taken into consideration. It is under the responsibility of Entities, Institutions and Corporations to conduct an asset assessment and to take actions according to degrees of significance of assets. In performance of penetration tests, it is required to use methods which do not lead to any service interruption or any suspension of activities of Entities, Institutions and Corporations. All tests which may cause service interruptions shall be planned and carried out in coordination with Entities, Institutions and Corporations.

(a) Access Points of Performance of Tests:

Minimum access points where penetration tests will be performed are defined and described below. Penetration tests shall be conducted after access to the system through these points.

i. Internet: Penetration tests shall be performed upon access via Internet to all servers and services of the Entities, Institutions and Corporations available via Internet, and thereafter, detailed penetration tests shall be conducted.

ii. Entities, Institutions and Corporations internal network: Penetration tests shall be performed upon access via internal network of the Entities, Institutions and Corporations to all servers included in internal network of the Entities, Institutions and Corporations and covered by the test. This network shall also be used for tests to be performed on the network and along the network traffic, and computers in the most commonly used user computer profile shall be supplied to persons assigned for performance of the test.

(b) User Profiles of Performance of Tests:

In order for penetration tests to be performed in a robust manner, and for the sake of conformity of tests to real life, penetration tests shall be performed on access points defined above in compliance with the nature of these environments by using the following user profiles.

i. Anonymous user profile: This profile represents a user who may access web services of Entities, Institutions and Corporations via Internet, but is not entitled to enter into web applications thereof. This profile should be used in order to detect threats that may be created for the system by users who are not members of web applications of Entities, Institutions and Corporations, and to eliminate the related weaknesses, and to find out required solutions for them.

ii. Entities, Institutions and Corporations customer profile: This profile represents corporate or individual users who may access web services of Entities, Institutions and Corporations and are entitled to enter into web applications thereof. This profile should be used in order to detect threats that may be created for the system by users who are members of web applications of the Entities, Institutions and Corporations on the Internet, and to eliminate related weaknesses, and to find out required solutions for them.

iii. Entities, Institutions and Corporations employee profile: This profile should be used in order to detect the authorities owned by staff of Entities, Institutions and Corporations by using the working environment, as well as the threats that may be created for the system by employees, and to eliminate related weaknesses, and to find out required solutions for them. In tests to be conducted by Entities, Institutions and Corporations employee profile, aside from selecting the most commonly used employee profile throughout Entities, Institutions and Corporations, penetration tests shall be performed also by using the profiles of employees having local administrator rights. In tests to be conducted by Entities, Institutions and Corporations employee profile, access authorities defined for and permissions granted to the person/entity performing the tests by Entities, Institutions and Corporations should be clearly stated.

iv. Other user profiles: If and when penetration tests are performed by a user profile which does not comply with the other four user profiles defined above, the rights and authorities defined for each profile used therein shall be clearly stated under this heading.

(c) System Detection, Service Detection and Vulnerability Scanning:

Penetration tests start with system detection, service detection and vulnerability scanning/research steps described below. System detection, service detection and vulnerability scanning/research shall be applied on all information system assets.

i. System detection: This is the step where system/configuration information of server or active/passive network devices are tried to be detected.

ii. Service detection: This is the step where assets included in information systems of Entities, Institutions and Corporations are subject to port scanning, and services offered by ports open to outer world/general access are tried to be detected.

iii. Vulnerability scanning/research: This is the step where the components of Entities, Institutions and Corporations and the services offered by these components are scanned for the currently available vulnerabilities by means of vulnerability scanners, and potential security vulnerabilities are tried to be detected. Additionally in this step, as for potential vulnerabilities detected, security effects and impacts of these vulnerabilities to components and to systems interacting with components shall also be researched by using such sources as vulnerability databases.

(d) Penetration Tests:

i. Basic penetration tests to be performed via Internet: System detection, service detection and vulnerability scanning steps shall be conducted from a location independent from the network of Entities, Institutions and Corporations by scanning the IP network owned by Entities, Institutions and Corporations on the Internet.

ii. Penetration tests to be performed from the Entities, Institutions and Corporations internal network: In the internal network of Entities, Institutions and Corporations, in addition to system detection, service detection and vulnerability scanning steps, the following activities shall also be carried out:

- Detection of corporate local network map;
- Performance of content filtering, firewall bypass and information retention tests over predetermined open ports;
- Performance of vulnerability scanning inside local area network;
- Trying to acquire information with a high degree of sensitivity by using man in the middle attacks in the corporate local network;
- In light of information collected as above, performance of capture attacks to user computers, server systems and active devices;

- Attempting to have access to more critical data and information through servers and user computers captured as above.

(4) Follow-up of Results of Penetration Test:

Entities, Institutions and Corporations follow up the findings detected as a result of penetration tests by taking into consideration the degrees of significance of findings, the probable risks that may be caused by them when combined, value of assets where these findings are detected, and suggestions given in the penetration test reports, within the frame of an action plan approved by the boards of directors of Entities, Institutions and Corporations and aiming to eliminate and resolve these findings as soon as possible. Detections made as a result of penetration tests are, if and when deemed necessary, included also in the internal audit plan of audit committees of Entities, Institutions and Corporations. Penetration test reports shall be sent to the Board within one month after they are completed.

Degrees of Significance of Findings:

Degrees of significance of findings shall be treated under five categories. These categories named as urgent, critical, high, medium and low are described in the following table:

Degrees of Significance	Description
Urgent	Vulnerabilities causing attacks by an unqualified attacker from the external network of Entities, Institutions and Corporations, resulting in the capture of the entire system.
Critical	Vulnerabilities causing attacks by a qualified attacker from the external network of Entities, Institutions and Corporations, resulting in capture of the entire system.
High	Vulnerabilities causing attacks from the external network of Entities, Institutions and Corporations, resulting in restricted privilege escalation or a denial of service, as well as vulnerabilities causing attacks from local network or via server and cause privilege escalation.
Medium	Vulnerabilities causing attacks from local network or via server resulting in denial of service.
Low	Deficiencies the effects of which cannot be fully and exactly determined, and which are caused by failure in application of the best hardening methods described in the literature.

Finding Format:

The formats for presentation of findings to be reported under each of headings listed in the Scope section are shown below.

Finding Reference No.	Letter/figure series individually describing each finding in the report:
Name of Finding	Descriptive name expressing the finding in summary
Degree of Significance	Degree of significance of the finding given in this Annex-1
Impact	Potential consequences of abuse of vulnerability/deficiency defined in the finding.

Access Point	Access point of performance of test indicated in “3.a Access Points of Performance of Tests” section
User Profile	User profile of performance of test indicated in “3.b User Profile of Performance of Tests” section
Component/ Components Where Finding is Detected	Such information as IP Number, URL, System, Service, Server or Asset name describing the component where the finding is detected
Finding Description	Detailed description of the finding
Suggestion for Solution	Suggestion for solution to be presented by the entity performing the test for elimination or resolution of the finding