REGULATION ON INFORMATION SYSTEMS AND ELECTRONIC BANKING SERVICES OF BANKS

Promulgated in the Official Gazette edition 31069 on 15.03.2020
Authority: Banking Regulation and Supervision Agency
Effective Date: 20.06.2020
Last Amendment Date: 20.06.2020
Effective Date of This Version: 20.06.2020

FIRST PART
Preliminary Provisions

SECOND PART
Establishment of Risk Management and Controls Regarding Information Systems

FIRST SECTION
Information Systems Governance

SECOND SECTION
Management of Risks of Information Systems

THIRD SECTION
Information Security Management

FOURTH SECTION
System Development and Change Management

FIFTH SECTION
Information Systems Continuity and Accessibility Management

SIXTH SECTION
Outsourcing of Services

SEVENTH SECTION
Information Systems Internal Control and Internal Audit Activities

THIRD PART
Electronic Banking Services

FIRST SECTION
Joint Provisions

SECOND SECTION
Internet Banking

THIRD SECTION
Mobile Banking

FOURTH SECTION
Telephone Banking

FIFTH SECTION
Open Banking Services

SIXTH SECTION
ATM Banking

FOURTH PART
Miscellaneous and Final Provisions

FIRST SECTION
Miscellaneous Provisions

SECOND SECTION
Final Provisions

Articles 13, 29, 40 and 42, and thirteenth paragraph and fifteenth paragraph of Article 34, and eighth paragraph of Article 37 of this Regulation will become effective as of 1/7/2020, and other provisions will become effective as of 1/1/2021.

FIRST PART
Preliminary Provisions

ARTICLE 1
Purpose and Scope

(1) The purpose of this Regulation is to set down the minimum procedures and principles to be employed in management of information systems used by banks in the course of performance of their activities and operations, and in provision of electronic banking services, and in management of risks relating thereto, as well as the information systems controls required to be established therefor.

ARTICLE 2
Grounds

(1) This Regulation has been prepared and issued in reliance upon Article 93 of the Banking Law no. 5411 dated 19/10/2005.

ARTICLE 3
Definitions and Abbreviations

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

a) "Open banking services" refers to an electronic distribution channel through which customers or parties acting for and on behalf of customers may execute banking transactions or may instruct the bank for execution of banking transactions through remote access to financial services offered by bank via such methods as API, web service, file transfer protocol, etc.; and

b) "Explicit consent" refers to an informed consent declared on a certain particular issue by free will and volition of the declarant; and

c) "API" refers to and stands for an application programming interface created so as to enable a software to use functions defined in another software; and

ç) "ATM" refers to and stands for electronic transaction devices allowing execution of not only automatic money withdrawal, but also all or a part of other banking transactions; and

d) "Bank" refers to any banks as defined in Article 3 of the Law; and

e) “Information systems (IS)” refers to human resources, operational activities and processes employed for collection, processing, storage, distribution and use of information, as well as information technologies which are in interaction with them; and

f) “Information systems continuity plan” refers to an information systems continuity plan as defined in Article 3 of ISEDES Regulation; and

g) “Information systems management” refers to activities with regard to effective, reliable and continuous conduct and management of activities performed and services offered by bank; and performance of obligations arising out of applicable laws and regulations; and establishment of an information systems environment fit and appropriate for assuring integrity, consistency, reliability, timely acquirability and attainability, and if needed, confidentiality of information procured from accounting and financial reporting system; and effective and efficient use of information systems resources; and control and monitoring of risks arising out of use of information systems; and systematic and managerial actions and measures required to be taken for the aforesaid purposes; and

ğ) “Information technologies (IT)” refers to and stands for hardware, software, communication infrastructure and other relevant technologies employed for input, storage, processing, transmission and output of data in any form or format; and

h) “Information assets” refers to both data used in performance of banking activities and operations, and all assets valuable for the bank such as systems, software, network devices, IT hardware and business processes employed for transportation, storage, transmission or processing of said data; and

ı) “Primary centre” refers to a structure wherein primary systems are built and established; and

i) “Primary systems” refers to primary systems defined in Article 3 of ISEDES Regulation; and

j) “Biometrical identity verification factor” refers to measurable biological or behavioural characteristics specific to an individual, employed for performance of identity verification transactions; and

k) “Outsourced services” refers to outsourcing for services which have access to banking data or where banking data are shared, and have the potential to impact confidentiality, integrity and availability of banking data

and continuity of banking services, and are outsourced by banks in respect of their information systems, also including the support services covered by the Regulation on Outsourcing for Services by Banks, promulgated in the Official Gazette version 28106 on 5/11/2011; and

l) "Electronic banking services" refers to all kinds of electronic distribution channels such as internet banking, mobile banking, telephone banking, open banking services, and ATM and banking kiosks through which customers can execute banking transactions remotely or can instruct the bank for execution of such banking transactions; and

m) "Electronic signature" refers to an electronic signature as defined in the Electronic Signature Law no. 5070 dated 15/1/2004; and

n) "Firewall" refers to hardware or software which assure control of traffic flow between networks having different security levels or between devices linked to network; and

o) "Sensitive data" refers to specific data that belong to customer and are kept and stored by bank, particularly data employed in identity verification, and if captured or acquired by third parties, may cause harm to mechanisms used for distinguishing the relevant individuals from other customers, and may smooth the way for fraud or swindling or fictitious transactions executed in the name of customers; and

ö) "Secondary centre" refers to a structure wherein secondary systems are installed and established ready for use, and which is designed so as to allow personnel to work and not to be exposed to the same risks with primary centre, in case of an interruption in primary systems; and

p) "Secondary systems" refers to secondary systems defined in Article 3 of ISEDES Regulation; and

r) "Internet banking" refers to electronic distribution channels through which customers can, independently from the device or platform used by them, reach and access via internet the services offered by banks through a web page under their own business name, company name or any other name, and customers can display or modify their own financial or personal data or can execute transactions leading to financial liabilities for them; and

s) "ISEDES Regulation" refers to the Regulation on Internal Systems and Internal Capital Adequacy Assessment Process of Banks promulgated in the Official Gazette edition 29057 on 11/7/2014; and

ş) “Business impact analysis” refers to business impact analysis defined in Article 3 of ISEDES Regulation; and

t) “Law” refers to and stands for the Banking Law no. 5411 dated 19/10/2005; and

u) “Interruption” refers to interruption of continuity in activities and operations of a bank, except for planned migrations; and

ü) “Identity verification” refers to a mechanism which provides assurance that an identity declared really belongs to the declaring individual; and

v) “Personal data” refers to and stands for personal data defined in the Personal Data Protection Law no. 6698 dated 24/3/2016; and

y) “Control” refers to all of the policies, procedures, applications and organizational structures employed in the course of IT processes in the bank and aiming to provide assurance of adequate degree in respect of achievement of business goals and objectives and prevention, determination and correction of undesired events; and

z) “User” refers to all types of users in whose name an account is identified for execution of transactions on bank’s information systems, such as bank personnel, external service provider employees or bank customers; and

aa) “Agency” refers to and stands for the Banking Regulation and Supervision Agency; and

bb) “Institutional SOME” refers to and stands for a Institutional SOME as referred to in Article 5 of the Communiqué on Procedures and Principles of Establishment, Functions and Operations of Cyber Events Response Teams promulgated in the Official Gazette edition 28818 on 11/11/2013; and

cc) “Board” refers to and stands for the Banking Regulation and Supervision Board; and

çç) “Mobile banking” refers to a customized internet banking channel that is uploaded on a mobile device such as smart phone or tablet and enables customers to execute their banking transactions via a mobile application of bank; and

dd) “Session” refers to a logical link established between the parties for data transfer, presentation or for financial transactions to be executed; and

ee) “Password” refers to a series of characters composed of secret letters, figures and/or special symbols, employed for identity verification purposes; and

ff) “Risk limits” refers to risk limits described in Article 38 of ISEDES Regulation; and

gg) “Sectoral SOME” refers to and stands for a Sectoral SOME established in the organization of the Agency as referred to in Article 7 of the Communiqué on Procedures and Principles of Establishment, Functions and Operations of Cyber Events Response Teams; and

ğğ) “Penetration test” refers to security tests conducted in order to detect and correct the security vulnerabilities of systems before they are abused; and

hh) “Cyber event” refers to a cyber event as defined in Article 3 of the Communiqué on Procedures and Principles of Establishment, Functions and Operations of Cyber Events Response Teams; and

ıı) “Cyber event response” refers to a cyber event response as defined in Article 3 of the Communiqué on Procedures and Principles of Establishment, Functions and Operations of Cyber Events Response Teams; and

ii) “SMS OTP” refers to and stands for a one time pad transmitted through short message service offered by electronic communication operators; and

jj) “One time password” refers to a series of letters and/or figures formed randomly for use only once for identity verification purposes; and

kk) “End-to-end secure communication” refers to transmission of data by sender with encryption decryptable only by recipient, for the sake of entailing only recipient to have access to the data communicated; and

ll) “Top echelon management” refers to top echelon management as mentioned and defined in Article 3 of ISEDES Regulation; and

mm) “Top management” refers to top management as mentioned and defined in Article 3 of ISEDES Regulation; and

nn) "Asset guard" refers to an individual who is responsible for protection of an information asset during its storage, transportation, processing or transmission, in accordance with the security requirements defined and set down by the asset owner; and

oo) "Asset owner" refers to an individual who determines and transmits to asset guards the security requirements of information assets and is liable and responsible for maintenance and accessibility of information assets by supervising and checking that security controls fit to these requirements are applied by asset guards; and

öö) "Patch" refers to a program add-on prepared for completion of security vulnerabilities detected in programs and for correction of faulty functions in the content of program.

SECOND PART
Establishment of Risk Management and Controls Regarding Information Systems

FIRST SECTION
Information Systems Governance

ARTICLE 4
Management Supervision, Roles and Responsibilities

(1) Bank board of directors is liable and obliged to handle management of information systems as a part of corporate governance practices, and to allocate financial and human resources required for correct management of information systems, and to ensure establishment of effective controls on information systems for the sake of confidentiality, integrity and availability of information assets, and to conduct an effective supervision for management of risks arising out of use of information systems by also taking into consideration the newly developed technologies. To this end, an IS strategy plan, an IS Strategy Committee and an IS Steering Committee approved by the board of directors are established. Bank board of directors may decide to combine strategy and steering committees by taking into consideration such criteria as bank's scale, its dependence on information systems, number of personnel, and external services outsourced for information systems. Job definitions and working principles of these committees are approved by board of directors.

(2) IS Strategy Committee is in charge of supervising in the name of the board of directors whether IS investments are used appropriately in line with

IS strategy plan or not, and whether bank's business targets are compliant with IS targets and goals or not, and reporting directly and regularly to the board of directors in connection therewith, and reviewing IS strategy plan at least once a year, and revising the same if and when needed, and presenting it to the board of directors for its approval, and supervising the activities of IS Steering Committee.

(3) At least one member of the board of directors is essentially required to enter IS Strategy Committee, and top echelon manager in charge of information systems and top echelon managers from the relevant business divisions of bank are required to be members of this committee. IS Strategy Committee meets at least twice a year in order to review whether IS strategy plan is regularly applied or not, and to assess the material and significant IS investment decisions, and reports to the board of directors at least once a year.

(4) An IS Steering Committee is formed and appointed in order to assist IS Strategy Committee and top echelon management in implementation of IS strategy in tandem with approval of the board of directors. IS Steering Committee is liable to determine the order of priority of IS investments and projects, and to follow up the progress of ongoing IS projects, and to resolve the conflicts of resources among projects, and to make the required guidance for the sake of compliance of IS architecture and IS projects with applicable laws and regulations, and to monitor service levels relating to IS services. IS Steering Committee is essentially required to be composed and comprised of representatives from IS, human resources and other relevant business units and divisions of bank, as well as representatives from the units or positions relating to compliance and law, if already included in the bank organization. IS Steering Committee meets at least twice a year and reports to IS Strategy Committee at least once a year.

(5) Comprehensiveness level of IS organization and information systems should be proportional to bank's size and complexity of its activities, and IS organization chart should also be designed accordingly. Duties, functions and responsibilities of all units within IS organization chart, and job definitions of personnel of these units are clearly written down, and are approved by board of directors or by top echelon managers delegated by board of directors therefor, and conformity of these job definitions is regularly reviewed.

(6) IS personnel are ensured to be aware of the job duties, functions and responsibilities assigned to them, and in case of change in their job duties, functions and responsibilities, to be made cognizant of such changes.

ARTICLE 5

Information Systems Policy, Procedure and Process Documents

(1) Bank issues IS policies, procedures and process documents describing the procedures and principles required to be applied, and the controls required to be established, with a view to managing the risks arising out of use of information systems and protecting the information assets.

(2) Right of access to documents is granted in proportion to the degree of confidentiality of documents and the relevance of duties, functions and responsibilities of bank employees. Documentation contains document code and document's degree of confidentiality at the minimum.

(3) IS policies are approved by board of directors, while IS procedures and process documents are approved by board of directors or by executives and managers delegated by board of directors therefor.

(4) Requirements of IS policies, procedures and process documents are incorporated and established in a workable and operable manner inside bank's organizational and managerial structures, and their functionality is supervised and followed up. Units and divisions responsible for operation of policies and procedures, and their job definitions, and process owners in charge of operation of process documents are clearly stated in the relevant policies, procedures and process documents.

(5) IS policies, procedures and process documents are reviewed at least once a year, and are updated if and when required. For the sake of following up the amendments and revisions made in the documents, such information as previous version of document, and individual approving the document, date of revision, and date of review are recorded and documented.

SECOND SECTION
Management of Risks of Information Systems

ARTICLE 6
Information Assets Inventory and Classification

(1) In order to establish and build controls fit to security requirements of information assets, bank classifies these assets and prepares a detailed asset

inventory. Asset inventory will contain the following data specifically for each information asset:

a) A definition clearly describing what asset is; and
b) Asset's relative value for bank; and
c) Current position of asset; and
ç) Asset's security class and such values as confidentiality, integrity and availability ensuring determination of said class; and
d) Owner of asset; and
e) Preservation of asset.

(2) In determination and assessment of value of information assets, business goals and business processes correlated with these assets are taken into consideration together with other business goals and business processes appertaining thereto.

(3) Data inventory to be formed and built for data being a part of information assets contains not only the details specified in first paragraph hereof, but also the information whether it is personal data or not.

(4) In collaboration with asset owners, each asset is ensured to have a defined and approved security class and access restriction. Security classes and access restrictions are regularly reviewed in periods not being longer than two years.

(5) Information Security Committee prepares and issues an approved asset classification guideline indicating how information assets may be classified. In determination of security class of assets, such criteria as degree of confidentiality, integrity requirements, availability requirements, period of storage, and minimum backup frequency are taken into consideration.

(6) Security class of data is determined by taking into consideration such criteria as degree of confidentiality, integrity requirements and availability requirements of data, as well as whether they are categorized as critical data, personal data or confidential data at the minimum.

ARTICLE 7
Information Systems Risk Management Process

(1) Bank establishes and employs an IS risk management process in order to analyse, mitigate, follow up and report the risks arising out of use of information technologies in its banking activities and operations.

(2) The following activities are carried out within the scope of IS risk analysis
a) Identification of risks through detection of threats and security vulnerabilities regarding information assets created within the scope of the first paragraph of Article 6

b) Determining the risk exposure possibilities of information assets according to the threats and security vulnerabilities detected,

c) Performance of an impact calculation correlated with the relevant information asset by determining the impacts of risks, if and when they occur, on such criteria as confidentiality, integrity and availability of the relevant information asset; and

ç) Making a risk rating of risks threatening information assets according to the probability and impact values determined as above; and

d) Preparation and presentation to top management of a summary risk assessment report corresponding to all of the works performed as a part of risk analysis.

(3) In respect of each of IS risks detected according to the risk analysis results, risk-related actions are determined in strict compliance with the value of information assets correlated with said risks and the bank's risk limits. At the stage of determination of risk-related actions, as a result of risk analysis, it will be decided together with representatives of relevant business unit how the concerned risks will be handled and managed by such methods as risk mitigation, risk avoidance, risk acceptance and risk transfer.

(4) Actions determined for each of risks as stated above are converted into a risk action plan. Transfer of resources for the actions to be taken as above, and prioritization of completion dates of actions will be based upon the risk degrees determined at risk analysis stage. Actions are planned also for residual risks remaining after implementation of action plan, and action plan is updated accordingly.

(5) A risk may be accepted only if and when it is duly approved by top echelon manager in charge of information systems, and does not contradict with IS strategy and applicable laws and regulations. If the risk to be accepted is at the same time correlated with a business process or business application, prior approval of top echelon manager of the relevant business unit is also required to be received as to acceptance of the subject risk. Risks accepted as above are periodically reviewed against the probability of subsequent emergence or development of new compensating control techniques or new

security solutions, or of change of conditions as to whether the subject risk has increased in comparison to before or not.

(6) Current risk assessment report and current risk action plan prepared as a result of risk analyses are combined to create an IS risk inventory. Bank repeats its risk analyses at least once a year or prior to material and significant changes in information systems. Risk action plan and IS risk inventory are ensured to be updated according to the repeated risk analysis results. Results of IS internal control and internal audit works performed in the bank, or findings detected therein are ensured to serve as inputs to risk inventory.

(7) Bank's corporate risk management process is essentially required to cover IS risks as well. Given that IS risks may further constitute a multiplier of other risks arising out of banking activities and operations, an integrated risk management methodology is applied in the bank as a whole, in such manner to cover also risks arising out of information systems. Data obtained out of outputs of IS risk management process are ensured to become a part of the bank's integrated risk management framework. In handling the risks arising out of information systems, risks brought by newly developed technologies are also separately assessed. Risks covered by IS risk inventory are followed up, and results are reported to board of directors and top echelon management at least once a year.

THIRD SECTION
Information Security Management

ARTICLE 8
Information Security Organization, Roles and Responsibilities

(1) Final responsibility of assurance of information security within the bank belongs to board of directors. Board of directors is under obligation to show the required determination for taking and implementing security measures in respect of information systems at the appropriate level, and to allocate adequate resources for the activities to be performed for that purpose. As a requirement of this responsibility, board of directors builds and establishes an information security management system the application of which in the bank in general is required to be supervised by board of directors. Information security management system is essentially required to take national or international standards or best practices as a reference, and to cover the following activities:

a) Performance of regular threat and risk assessment works and activities in correlation with information assets; and

b) Classification of information assets, and determination of asset owners, and taking of security measures fit to asset classes; and

c) Monitoring and reporting of events and incidents in respect of breach of information security; and

ç) In the course of banking services provided by the bank in general, ensuring establishment of an effective identity verification and access management consistent with the principle of segregation of duties; and

d) Testing the controls and structures built for the sake of information security, and monitoring and reporting the test results; and

e) Ensuring that current security vulnerabilities affecting information assets are followed up, and the required actions are taken in relation therewith; and

f) Performance of works aimed at raising information security awareness in bank for bank employees, also including top management, and for stakeholders related to bank's information security, such as external service providers and customers; and

g) Ensuring that issues correlated to information security are also covered by and included in business continuity management; and

ğ) Ensuring that issues correlated to information security are also covered by and included in management of outsourcing for services.

(2) How the information security management system will be applied in the bank in general is to be determined and regulated by information security policies, procedures and process documents. Bank's information security policy is approved by board of directors, and is ensured to be circulated to all employees of bank. To this end, acceptable standards of use are determined in respect of information systems.

(3) Information security policy is formulated and applied by Information Security Committee in the name of board of directors. Information Security Committee is chaired by a designated director or general manager, and is coordinated by information security supervisor. Meetings of Information Security Committee are required to be attended also by top echelon manager

in charge of information systems, and top echelon managers from the relevant business units of bank, and representatives from human resources and risk management units, and if available in bank organization chart, from units or positions related to compliance and law as well. Job definitions and working principles of Information Security Committee are written down upon approval by board of directors, and the Committee is ensured to meet at least twice a year and to report to board of directors at least once a year.

(4) Information security policies, procedures and process documents are reviewed at least once a year. They are ensured to be separately reviewed also after material security incidents, new security vulnerabilities or material changes in technical infrastructure.

(5) Within bank organization, an IS security function is formed and organized separately and independently from IS function comprised of top echelon manager in charge of information systems and of units reporting to him. IS security function is essentially required to report directly to board of directors or general manager. Bank's IS security function is managed and directed by information security supervisor.

(6) Information security supervisor performs the following job duties and functions:

a) Preparation, updating, and presentation to approval, of information security policies, procedures and process documents; and

b) Classification of information assets from the perspective of information security, and providing active contribution to and assistance in IS risk management works and activities in terms of confidentiality, integrity and availability criteria correlated with information assets; and

c) In harmony and collaboration with the relevant units, establishment of information security in the bank in general in compliance with business requirements and business goals; and

ç) Following up and monitoring the compliance with applicable laws and regulations, standards, policies, procedures and process documents with regard to information security; and

d) Ensuring that information security activities and tests are carried out, and following up such activities and tests; and

e) Making contribution to the works for determination of information security requirements in respect of material projects and changes; and
f) Conduct of bank's information security awareness program for its stakeholders in respect of information security.

ARTICLE 9
Data Confidentiality

(1) Bank takes all actions and measures needed for keeping data in strict confidence in all media and environments where data used in performance of banking activities are carried, transmitted, processed, kept and backed up. Independently from the media used for keeping said data being paper or electronic, the actions and measures taken are essentially required to be in conformity with degree of confidentiality of data intended to be kept confidential, and if and when needed, all required additional controls should also be built therein. If and when data hosting media or devices are out of use, data contained therein are ensured to be securely destroyed in accordance with their degree of confidentiality.

(2) For encryption techniques to be used for the sake of confidentiality of data, algorithms which have not lost their reliability and are in conformity to the currently available technologies under the current situation are used. Encryption keys to be used are selected so long that they cannot be broken during the time the keys will be valid and may be used for the relevant algorithms, and validity time of these keys is determined according to the criticality level of the relevant data or operation. Use of an encryption key of which validity time expires or which is detected to have lost its reliability is promptly prevented. Encryption keys are essentially required to be kept secure throughout their life cycle, and to be formed securely, and to be presented to the use by customers and personnel, and to be stored.

(3) In transmission of sensitive data between the media having different security levels, end-to-end secure communication is essentially required to be used, and such data are to be kept encrypted. Contents of all desktop, laptop and mobile devices containing sensitive or confidential data and information and allocated by bank to its personnel are ensured to be encrypted, and server machines are scanned to determine whether sensitive data are available in public text form on the server devices linked to network or not.

ARTICLE 10
Sharing of Data

(1) Without a customer request received from the customer itself in writing or via permanent data storage units in a verifiable manner, and except for the pertinent provisions of the Law, bank is not allowed to share with or transfer or disclose to third parties resident at home or abroad any of the information classified as confidential information of customer and acquired, stored or processed by bank through information systems during and in the course of performance of its activities and all kinds of outsourcings hereunder.

(2) Explicit consent to be given by customer for sharing of its data and information can by no means be formulated as a condition precedent for provision of the relevant banking services.

ARTICLE 11
Identity and Access Management

(1) Bank is under obligation to make sure that access to information assets is managed by an identity verification method convenient and suitable for security class of the relevant information asset, pursuant to access controls determined according to the principle of segregation of duties and defined for users themselves as per their personal responsibilities. Bank ensures that the authorizations to be provided to users over processes and systems are granted to users through roles and/or profiles fit to their job duties and responsibilities, and documents the roles on systems and applications in conformity with job definitions of users.

(2) Identity verification mechanism to be applied to users over information systems is to be established so as to cover the process from incorporation of users into information systems to the time they complete their transactions and depart from the system, and measures are taken in order to guarantee the accuracy of identity verification data from the beginning to the end of session.

(3) For security of identity verification data of users over information systems, bank takes such measures as storage of identity verification data in databases through encryption or other methods which cannot be reversed mathematically, and encryption of identity verification data while they are transferred for identity verification purposes, and protection of such data against unauthorized access or changes that may be attempted to be made in an uncontrolled manner in contradiction with the principle of segregation of duties, and keeping of adequate logs regarding transactions performed on said databases, and keeping these logs secure.

(4) Identity verification mechanism to be applied to users is ensured to perform the following functions:

a) Prevention of access by the relevant user if and when unsuccessful identity verification attempts excess a certain predetermined number; and

b) After unsuccessful identity verification attempts, with respect to wrong user name or password data entered into the system, the attempter is not informed that such a user name is not registered in the system, or the password entered is wrong; and

c) As for dormant sessions without any transaction or movement, the session is terminated or locked after a certain time; and

ç) Unless the information security supervisor gives approval for use of the same user account by more than one user or for opening of different sessions by a user at the same time, if and when it is attempted to open more than one session for the same user at the same time, it is by no means permitted, and the user is warned thereabout.

(5) The principle of segregationof duties is relied upon in determination of access controls to be applied to and of authorizations to be assigned to users. Processes and systems are designed and operated in such manner not to allow initiation, approval and completion of a critical transaction by a single individual. Bank clearly determines and documents the access controls to be applied to and of authorizations to be assigned to users in banking and IS processes with a view to ensuring application of the principle of segregation of duties. The duties of requesting, authorization and management of access powers are ensured to be separated from each other. Where it is not possible to separate the duties from each other in the strictest sense and appropriately, additional risk mitigating or compensating controls are established in order to prevent errors and frauds that may be caused thereby.

(6) Users are authorized to access to information assets during the time a valid business need exists and access thereto is required. Users having an authorization of access to information assets are reviewed by the relevant information asset owner at least once a year. Considering their job duties and responsibilities, the users are ensured to be authorized to access on need-to-know basis only to data and information which are adequate and they need to know for fulfilment of their relevant duties.

(7) The following measures are ensured to be taken at the minimum in respect of users and application accounts having privileged powers:

a) Application of additional security controls together with identity verification; and

b) Assignment of privileged authorizations only to the required users and use of these types of accounts only if and when needed; and

c) Keeping of logs in such manner to follow up the transactions executed with these types of accounts, and regular review of them; and

ç) Keeping of logs and generation of warnings for transactions such as account creation or deletion; and

d) Keeping of logs and generation of warnings for unsuccessful entry attempts; and

e) Prevention of shared use of accounts or use of techniques for assignment of responsibility to natural persons using these accounts; and

f) Making configurations for the sake of storage of passwords in secure environments and for change of passwords in certain periods; and

g) Frequent change of passwords in such manner to create passwords difficult to be estimated and being of a length and difficulty in conformity with the current technologies; and

ğ) Where logs of application accounts cannot be created, kept or followed up due to systematic reasons, prevention of use of these accounts by end user.

(8) Authorizations for emergencies are made temporarily, and logs are ensured to be kept in such manner to allow follow-up of the transactions to be executed during the validity of said authorization.

(9) After changes in human resources such as resignation of personnel from job or change of duty or position, such transactions as deletion and suspension of the relevant user accounts, and withdrawal or change of authorizations assigned to users are performed without delay. Where the authorizations based upon changes in human resources are not performed automatically, the principle of segregation of duties is applied in the course of manual change process, and logs regarding activities of personnel authorized to make changes are regularly reviewed in terms of compliance with the changes in human resources.

(10) For users over information systems, unique user identification codes are determined, and shared or default user accounts are not used as long as it is not obligatory. Where it is obligatory to use shared or default user accounts, additional controls are established in order to assign responsibility to the personnel executing the transaction with such user accounts.

(11) At least following measures are ensured to be taken in management of user passwords:

a) To ensure that passwords given temporarily by the system are changed by user at the time of first login to the system; and

b) To force the users to choose passwords difficult to be estimated and of a length and difficulty in conformity with the current technologies; and

c) To force the users to change their passwords in regular intervals and whenever a doubt arises in respect of system security; and

ç) To preclude the uses from using their old passwords of a certain number retrospectively by remembering their old passwords.

(12) As for user accounts, bank uses methods automatically generating reports for and on locked accounts, deactivated accounts, accounts with an expired password validity time, and accounts the password expiry time of which is adjusted so as not to expire ever, and transmits these reports to the relevant system manager for the necessary measures required to be taken therefor.

(13) Bank personnel or external service providers are prevented to have local administrator rights except for a mandatory business requirement and unless approved otherwise by information security supervisor.

(14) Bank creates typical account usage profiles by determining a normal daily use and access time for each user. These usage profiles are used in detection of extraordinary situations through reporting of users who enter the system at unusual hours, exceed normal entry time, or execute a transaction via a computer other than the computer generally used by them, or in detection of passive accounts showing no activity since a long time, and if there is no more any business requirement for these types of accounts, prevention of use of these accounts.

ARTICLE 12
Integrity Checks

(1) Bank assures accuracy, correctness, completeness and reliability of transactions, records and data over information systems by taking actions and measures needed for protection of their integrity. Actions and measures for protection of integrity are taken and established so as to cover all of the stages of transmission, processing and storage of data. The same approach is adopted also for the transactions executed in external service providers.

(2) Accuracy, correctness and reliability of transactions on information systems require, at the minimum, the information of key importance correlated with the intended transaction to keep and maintain its accuracy and correctness from the beginning to the time of completion of transaction, and the intended transaction to produce and yield the results expected from it, while completeness of transactions on information systems require, at the minimum, that all subject transactions are executed faultlessly and without any redundancy or duplication.

ARTICLE 13
Formation and Follow-up of Logs

(1) Bank establishes and employs an effective logging mechanism regarding transactions and events performed within the information systems in proportion to size and complexity of information systems and activities. Logs contain at least the following information in details and with contents fit to the nature of the underlying transaction:

a) System generating the record; and
b) Date, time and time zone of generation of record; and
c) Information pointing out the change, together with the transaction or event generating the record; and
ç) Information indicating individual user or system correlated with the record.

(2) Logging mechanism to be established as above is ensured to allow subsequent investigation of information security events and collection of reliable evidences and proofs about them.

(3) Logs relating to transactions executed within information systems and leading to changes in records about banking activities, and transactions aiming to access to critical or confidential data or to inquire, display, reproduce, copy or change the same, and activities aiming to grant, change

and withdraw powers and authorizations of access to critical information assets, and unauthorized access attempts to said assets are kept by the bank for a minimum period of five years.

(4) Logs regarding interrogations made by bank about the data kept in other institutions or entities through web services, API or similar other methods, and purposes of said interrogations are kept in bank for a period of five years, and logs of these interrogations are reported in monthly periods at the latest, and it is checked whether unauthorized or out-of-purpose interrogations are made or not, and the required actions are taken for the results obtained out of this checking.

(5) Logs are backed up in reliable media, and are kept in bank in such manner to allow retrieval and examination of these backup records within a reasonable time if and when needed.

(6) Techniques permitting prevention of impairment of integrity of logs and detection of any impairment upon occurrence are employed. Logs are made accessible only by individuals having the authorization to access thereto in accordance with the need-to-know principle, and recording system is ensured to be protected against all kinds of unauthorized changes, modifications or interventions. Users are precluded from intervening logs correlated to their own activities, and techniques aiming to prevent stoppage of log system and to detect any stoppage upon occurrence are employed.

(7) Bank establishes processes regarding regular review and follow-up of logging system within the frame of scenarios updated in certain predetermined periods, and reporting of extraordinary situations and risky transactions. Reports are ensured to be produced about extraordinary situations and risky transactions, and report results are ensured to be followed up by bank audit units and officers.

(8) Bank assures compliance of logs kept by external service providers with its own standards, and accessibility of these logs by bank.

ARTICLE 14
Network Security

(1) Bank establishes the required network security control systems for threats coming from both its own corporate network and other external networks. In establishment of security measures, a stratified security architecture is employed wherein if and when a security layer is surpassed, the other security layer steps in.

(2) Bank uses systems, compliant to current advanced technology, which are configured as required for keeping the traffic between its external network and internal network under control, and can detect and prevent attacks by firewall solutions kept continuously under supervision.

(3) Bank's internal network is divided into sub-segments in such manner to ensure that traffic of each service included in bank's internal network can reach only the network segments needed for itself, in order to mitigate impacts of probable threats coming from internal network and to assure controlled passage by separating sub-segments of bank's internal network having different security sensitivities from each other. Security of data traffic among different network segments is maintained. Only authorized devices are allowed to link to internal network.

(4) Systems having critical or confidential data are ensured to be hosted only in internal private network, and not to be ever accessible directly via internet. Communication is established with systems contained in internal private network only through proxy applications or firewall devices.

(5) Structures such as domain management servers built on network for identity and access management purposes are essentially required to be established specifically for bank, and not to be a part of another domain or similar units outside the bank.

(6) Connections made to critical network segments are regularly determined, and a needs assessment is performed for each of these connections, and unnecessary connections are ensured to be terminated.

(7) Unless specifically approved by information security supervisor, bank personnel or external service providers cannot have remote access to bank's internal applications and systems from outside bank. In case of remote access, secure connection methods based on multicomponent authentication are applied, and logs of accesses are kept, and duration of connections and devices that can be used for connection purposes are restricted, and user is forced to re-verify his identity in certain time intervals.

(8) Servers and systems which are visible via internet or through bank's external network are regularly checked in order to determine whether there is still a business need requiring them to be visible or not, and if not needed any more, these servers and systems are ensured to be moved to bank's internal network and to have internal network IP addresses.

(9) Bank checks and controls contents of traffic flowing from its internal network to external network. The content control is ensured to be capable of preventing traffic flow towards malicious IP addresses and leakage of critical data and confidential data, and of recording the session data and detecting the extraordinarily prolonged sessions and generating warnings for them.

(10) For e-mail messages sent from bank, techniques are used for verification of identity of sender in e-mail servers.

ARTICLE 15
Security Configuration Management

(1) Bank produces hardened and tested secure standard configuration information for operating systems, databases and applications on desktop, laptop and mobile devices and servers and for network devices such as firewalls, routers and switches. Such standard configuration information, deviations from standard configuration, or updates in standard configuration are recorded as a part of change management and made subject to an approval mechanism. For all kinds of change requests remaining outside the secure standard configuration, such information as business requirements requiring such change, and identity of business supervisor in need of these business requirements, and duration of business requirements are recorded.

(2) In addition to the controls mentioned in the preceding first paragraph, bank applies a white list for applications that are used or may be needed by it. Thus, only the needed applications are ensured to be uploaded in systems, and any application outside this white list is prevented to be uploaded to or operated in systems. At the same time, bank conducts regular scanning to check whether any application not included in white list is uploaded in its systems or not. Whether operable files of applications in white list or library files used by them are replaced via malicious software or not is checked by using file integrity control tools.

(3) For operating systems on desktop, laptop and mobile devices and servers, bank keeps a software inventory containing a list of type, version number and patch level of these operating systems, and of databases and applications uploaded on them. Software inventory to be used is ensured to be also integrated to hardware inventory at the same time, information as to which software is uploaded in which hardware are ensured to be traceable from one single point.

(4) Bank’s desktop and laptop machines and servers are configured and structured in such manner not to automatically move or play its contents

when any portable media or external device is fixed to these machines, and malicious software prevention tools are adjusted so as to automatically scan and check these devices when they are fixed thereto. In addition, connection interfaces through which such types of external devices are to be connected to machines are ensured to be deactivated as default, and these types of devices are allowed to be used only by users having business requirements therefor, and situations of attempts of use of external devices are also ensured to be followed up.

(5) Ports, protocols and services on each system linked to network are ensured to be open and operating only in reliance upon preapproved business requirements. Accordingly, port scanning is performed regularly for material and significant servers and systems on the basis of a secure base configuration, and ports that are in open position though not being in a secure base configuration are ensured to be closed.

ARTICLE 16
Security Vulnerabilities and Patch Management

(1) In order to reduce the probability of emergence of incidents which may interrupt or make material negative effects on banking activities, a security vulnerabilities and patch management process which can quickly and effectively handle and manage security vulnerabilities in systems, software and devices is established therein. Activities carried out as a part of security vulnerabilities and patch management process are recorded as a part of change management, and are subject to approval mechanism. The following activities are conducted under this process:

a) Use of techniques which ensure and verify that patches to be applied are coming from a reliable source; and

b) Detection of security vulnerabilities contained in systems, software and devices used by bank, and of patches for these vulnerabilities; and

c) Assessment of impacts of application or non-application of patches detected as above; and

ç) Pre-application testing of patches to be applied; and

d) Description of methods of application of patches; and

e) Regular reporting to information security supervisor in respect of patches applied or decided not to be applied; and

f) Definition of methods to be applied for solution of problems that may be faced due to wrong application of patches or during application of them; and

g) Establishment of compensating controls aiming to mitigate risks relating to security vulnerabilities tried to be addressed by patches that cannot be applied.

(2) If and when specific systems, software and devices the supplier or manufacturer support of which expires can no more be updated, and the recent updates that can be uploaded for them are no more secure according to the then-available circumstances, and security cannot be provided at a reasonable level also by compensating controls, then and in this case, such systems, software and devices are ceased to be used.

(3) Bank employs automatic security vulnerability scanning tools for its systems and devices linked to network. In respect of each security vulnerability detected, a report listing the most critical security vulnerabilities with priority is submitted to both the information security supervisor and the system manager in charge of the system where subject vulnerability is detected.

(4) Bank is under obligation to continuously monitor its desktop and laptop machines and servers, and to detect malicious software loaded therein.

(5) Bank further employs solutions which scan and check e-mail messages incoming to and outgoing from e-mail server, and prevent e-mail messages which host a malicious software or contain adds-on unnecessary in the light of bank's business requirements.

ARTICLE 17
Physical Security Controls

(1) Critical information systems are hosted in such secure areas as data centres, system rooms and network equipment rooms having appropriate security barriers and entry controls. Access to these areas is limited only by personnel required to have an access, and accesses are regularly reviewed, checked and updated.

(2) In selection of locations of data centres, bank takes into consideration natural risks and environmental threats correlated thereto. Buildings are ensured not to carry signs and information which give out the existence of data processing installations hosted therein.

(3) Bank uses systems and sensors for monitoring such environmental conditions as power failures, fire, smoke, temperature, water, dust and humidity which may negatively affect operation of data centres, and keeps them regularly maintained.

(4) Except for personnel specifically authorized under first paragraph hereof, any bank personnel, visitors, external service suppliers or contractor personnel may have access to data centres and critical information systems only subject to a prior approval mechanism, and their activities are closely monitored during their works in data centre, and they are absolutely accompanied therein. Logs are kept about requests and approvals for access to data centres and system rooms, and about transactions and entrances and exits under such accesses. For these areas, camera surveillance and recording systems are used with no blind spot therein and so as to keep records for at least one year. Views recorded by camera surveillance and recording systems are ensured to be backed up in a different position.

ARTICLE 18
Cyber Event Management, Penetration Test and Cyber Intelligence Sharing

(1) Bank establishes and implements a cyber event management and cyber events response process aiming to handle, manage and follow up cyber events in order to rectify and normalize IS services as soon as possible and in such manner to make minimum impact on banking activities after cyber events. A Institutional SOME having adequate technical and operational skills is ensured to be appointed, and current communication and contact data of such Institutional SOME are transmitted to the Agency, and cyber events are ensured to be reported to the Agency and relevant management units.

(2) Institutional SOME is, prior to a cyber event, under obligation to conduct or cause others conduct routine penetration tests on IS assets, and to routinely monitor and follow up logs through log management system interface, and to control correlations that may create meaningful results among logs, and during a cyber event, is liable to manage the response to be done by IS function, and to coordinate the relevant personnel assigned in IS function.

(3) In order to make sure that cyber events are handled and managed in accordance with their significance levels, criteria pertaining to significance and materiality classification of cyber events are documented, and procedures and response plans are produced so as to ensure that each cyber event is

handled and resolved within a period of time proportionate to its significance level determined according to said criteria. For scenarios contemplated in response plans produced as above, a quick, effective and regular reaction process ensuring that activities are continued and carried out in a reliable manner is established. Functionality of response plans is tested at least once a year, and test results are reported to top management.

(4) Within the response plans, processes aimed to quickly find out the source of event relating to information systems, to reach authorized units, to determine potential size, impacts and damages of event and customers affected therefrom, and to resolve the event are arranged.

(5) In the event that a cyber event grows up and transforms into a crisis, and results in leakage or disclosure of data, and therefore, Information Systems Continuity Plan or secondary centre is activated, bank immediately reports to Sectoral SOME. In case of occurrence of a cyber event leading to leakage or disclosure of sensitive data or personal data, customers are informed thereabout after an assessment to be performed by the bank.

(6) For significant cyber events causing serious interruptions or failures in IS services, bank is under obligation to conduct a root cause and impact analysis and to take remedial measures aiming to prevent repetition of similar events and to report the works to Sectoral SOME.

(7) Bank causes a penetration test to be performed at least once a year by independent teams not involved in or assigned for design, development, implementation or performance of services offered through information systems.

(8) Bank is further liable to give information about new cyber threats, malicious software, cyber events or new fraud methods emerging in banking sector which are detected by it or come to its knowledge, and to appoint a contact person communicable on 7/24 basis so as to ensure early response in the course of anti-fraud operations, within the frame of procedures and principles to be determined by the Agency.

ARTICLE 19
Increasing Awareness on Information Security

(1) A comprehensive information security awareness training program is created and implemented in order to increase information security awareness level all over the bank. Training program contains information about individual responsibilities correlated to information security and data

protection, and about measures required to be taken for protection of information assets, together with information security policies and standards. Through these training activities, everyone having right of access to IT resources and systems of bank are ensured to be informed about the laws, regulations and directives in respect of use of these resources.

(2) Information security awareness training program is approved by Information Security Committee, and contents of program are reviewed and updated at least once a year by taking into consideration new technologies and newly emerging risks. New and existing personnel having right of access to bank's IT resources and systems, and external service providers having right of access to bank's IT resources and systems in line with the areas they are involved in are ensured to attend these training activities or document and prove that they have already taken such training, and as the training program is updated, relevant individuals are ensured to be retrained about the updated parts thereof.

(3) In order to increase information security awareness level, in addition to training program, bank prepares and issues in-house bulletins, and creates a section relating to information security in bank's internal portal, if any, and periodically sends information security reminder messages to its employees, and organizes regular surveys and polls for its employees for measurement of information security awareness level.

(4) Bank conducts all works and activities required for verification of efficiency of awareness increasing works covered by this article and for detection of deficiencies and weaknesses required to be improved. By taking into account current attack methods, bank performs periodical tests on its employees over the required social engineering scenarios, and ensures that its employees failing in these tests take additional trainings directed to certain targets.

FOURTH SECTION
System Development and Change Management

ARTICLE 20
Defining Information Architecture

(1) Bank relies upon a corporate information architecture model which assures integrity and consistency of data to be processed and stored through information systems and minimizes data redundancy therein.

(2) As a part of information architecture model, bank determines data syntax rules, and creates a data dictionary describing standard structures required to be abided by data in tandem with these syntax rules, and ensures use of this data dictionary in the course of software development and database management processes. Data inventory built under Article 6 is ensured to be integrated to information architecture model.

(3) Related responsibilities are assigned for central follow-up and management of information architecture model, data syntax rules and data dictionary, and approval of responsible supervisors is taken for changes in applications or databases affecting architecture, and such changes are ensured to be updated through reflection onto information architecture model.

ARTICLE 21
Project Management

(1) Bank implements a project management process in order to ensure that IS projects are prioritized and coordinated correctly, and that information systems to be acquired or developed through these projects are delivered in a timely manner and with the required functionality level. Project management process assures establishment of an appropriate management structure according to size, complexity and riskiness of subject projects.

(2) Concrete criteria as to which types of works will be classified as project and how they will be prioritized are defined, and project requests are handled within the frame of said criteria for the sake of operation and supervision of the projects.

(3) Process at least covers the steps of determination of project needs and requirements, and determination of roles and responsibilities, and timing and resource planning, and description of details of activities to be carried out under the project, and definition of project stages and outputs, and determination of key dependencies, and quality assurance, risk assessment and approval.

(4) At the step of determination of project needs and requirements, an analysis document describing the requirements in details is prepared and issued. This analysis document enumerates and lists the legal requirements throughout the project life cycle, and security and confidentiality

requirements such as identity verification, authorization, access controls, approval mechanisms, encryption and logging, and performance requirements such as expected intensity of use and number of users, and accessibility requirements such as service levels and backup order.

(5) Bank prepares a project plan for IS projects, and project plans indicate the outputs to be derived and the milestones targeted to be reached at each stage of project. In order to ensure that the milestones cited in project plans are reached and the delivery is realized in a timely fashion and to manage the project risks, bank tracks and follows up the progress of project, and if needed, ensures that information is given to IS Steering Committee about progress of projects and problems encountered therein.

ARTICLE 22
System Development, Migration and Installation

(1) Bank ensures that development, testing and production environments are kept separate from each other in accordance with the principle of segregation of duties in the course of software development process. Systems and applications development process is run and operated in accordance with the principle of segregation of duties in such manner not to allow source codes to be prepared and edited by a single person and to be transported or moved among development, testing and production environments.

(2) Only for a valid business need and in case of absolute necessity and only after completion of a prior approval mechanism, personnel in charge of software development may be permitted to have access to production environments. Even in such circumstances, the acts performed by personnel in production media are followed up and recorded. Bank records and documents the methods employed in access to production environments, and ensures that such methods are approved by top echelon managers.

(3) Stages of software development process of bank, and transition conditions, documentation requirements and coding standards correlated to those stages, and at which stages business units and other stakeholders will be involved in the process, and at which stages their approvals will be taken are written down and documented. In the course of software development process, bank is ensured to strictly comply with software development life cycle, legislative requirements and internal policies, also including the process of outsourcing for services.

(4) With a view to increasing software quality and minimizing the security vulnerabilities, information security is carefully handled in software

development life cycle. Starting from the beginning of software development or supply process, besides determination of business requirements and functional requirements expected from software, security-related requirements such as authorization and access, identity verification, data integrity, logging and exceptional case management are also determined, and whether they comply with the bank's security standards, policies and legislative requirements or not is checked.

(5) Applications open to internet either developed in the bank or procured from outsources are scanned and checked for security vulnerabilities before they are installed and in a regularly repeated style after each of updates made in those applications.

(6) By taking into consideration the criticality and riskiness of outsourced services and the probability of cession of business by supplier, for applications the software of which is developed by an external supplier and the source code of which cannot be procured, a software storage agreement is to be signed with participation of third parties as well. Product updates and program debugging are also ensured to be covered by this software storage agreement.

(7) Bank ensures that its software development personnel take secure code development training specifically for software development environments they use.

(8) Consistency of new data definitions made in the course of bank's software development process or changes made in data definitions with information architecture in terms of data dictionary is assessed and checked, and if need be, the required updates are ensured to be made.

(9) In order to prevent addition of unauthorized or malicious code snippets into software codes during transportation of them among development, testing and production environments, integrity checks based upon versioning and release controls are performed. Approvals of the relevant users or application owners are taken at the time of transfer to production environments.

(10) Testing environment is ensured to represent production environment in terms of operating system, database management system, integrated applications and systems, and test data are ensured to represent operations carried out in production environment in terms of number and nature, and to be cleared of production environment data belonging to customers.

ARTICLE 23
Application Controls

(1) Applications developed by bank or procured from external suppliers host and contain systematic or manual controls aiming to conduct the relevant banking activities and business processes in accordance with bank's internal policies and legislative requirements, and to assure accuracy, completeness and reliability of data entered into these applications and changed, processed or produced by said applications. These controls assume and perform such functions as definition of data serving as inputs to the application, and control of kinds, types, formats and sizes of them, and verification of source thereof, and assurance of integrity and reliability of data processed by the application, and authorization of access to data in accordance with the principle of segregation of duties, and if need be, establishment of input – approval structure, and assurance of confidentiality, integrity and reconciliation of data serving as outputs of application and distribution of such output data only to the relevant parties. Bank makes sure that application controls are as far as possible systematic controls and are not conducted by manual routines, and prior to installation of applications, bank tests the controls hosted therein so as to make sure that they are in compliance with bank's internal policies and legislative requirements, and records the test controls.

ARTICLE 24
Change Management

(1) Bank establishes and implements an effective change management process which minimizes the number and impact of errors and problems that may emerge due to the changes, and ensures that changes are realized and completed efficiently, quickly and in a controlled manner, and actions and transactions effected during changes are auditable also after the related change. All kinds of changes to be made in information systems components such as network infrastructure, hardware, operating systems and software, and system, service, application configurations and parameters are ensured to be initiated within the frame of change management process, and change request is ensured to be relied upon a valid business need and requirement, and to be authorized, tested, realized, recorded and documented in accordance with the principle of segregation of duties. Changes are essentially required to be made by authorized users the identity of whom is verified by appropriate techniques, and adequate logs are required to be kept for them, and logs kept as such are required to be reviewed regularly.

(2) Bank keeps records of main version of information system software components, and records the changes in information system components according to chronological order and together with the date of change.

(3) Change management process covers at the minimum the steps of request management, risk assessment, concerned authority approval, and application, testing and verification of the change made. Accordingly:

a) Change requests are ensured to be recorded, and only change requests received from authorized persons are accepted, and a risk and impact analysis is conducted in relation therewith, and received requests are classified and prioritized.

b) In order to make sure that changes do not cause a security vulnerability, inspection activities which give an as high as possible assurance, also including source code inspection, are performed.

c) Changes are tested in line with appropriate test plans, and approvals of users and relevant units are taken before the changed modules are incorporated into and transferred to production environment.

ç) In order to minimize the risks correlated to changes, in line with the results of change management process risk assessment, prior to change, the systems or applications to be effected from change are backed up, and a retrieval plan is created and built so as to be able to return to an old version of the relevant systems or applications if and when a problem is encountered during or after transfer to production environment.

d) After changes are realized, the required updates are made so as to reflect changes also in the system and user documents and procedures such as operational procedures, configuration data, application documentation, help screen and training materials.

(4) Approvals that cannot be taken or documents and records that cannot be kept in the course of normal operation of process due to exceptions not defined in change management process as a part of emergency changes are ensured to be completed as soon as possible after change.

FIFTH SECTION
Information Systems Continuity and Accessibility Management

ARTICLE 25
Primary and Secondary Systems

(1) Banks are essentially required to host their primary and secondary systems domestically.

(2) All and any backups of primary systems, regardless of the rank or order of that backup of primary systems, are accepted and treated as secondary systems and are subject to the proviso of first paragraph hereof.

(3) Such systems as bank's internal messaging systems and market monitoring platforms which do not have the responsibility of conduct of banking activities or performance of responsibilities referred to in the Law and other applicable laws and regulations are not included in and treated as primary systems. In order for any system or application used by the bank not to be included in and treated as primary systems, any business process is required not to be conducted over that system or application, and data which may be categorized as critical data or confidential data are required not to be processed, transmitted or stored therein or thereby.

(4) Except for such banking transactions or payment or messaging systems in strict need of interaction with abroad by their very nature, bank should essentially be able to effect banking transactions without being subject to any approval process of a system established abroad, and even in case of interruption of its links with foreign communication networks, be able to continue offering its banking services and performing banking transactions at home through its primary and secondary systems built and established at home.

(5) In case of receipt of external services or cloud computing services for an activity covered by primary or secondary systems, information systems used by external service product to execute activities regarding its services and their backups are also handled and managed as a part of primary and secondary systems and are hosted and kept at home.

ARTICLE 26
IT Operations Management

(1) Bank runs and operates an IS operation management function performing daily management and maintenance duties of IT infrastructure in order to make sure that IS services are offered and provided in accordance with predefined service levels. Service levels of these services are defined with participation and approval of relevant business units in strict compliance with targets and business requirements set down in IS strategy plan.

(2) Bank further establishes a help desk function and a problem management system in order to immediately respond to IT operational events, and give support to users in resolution of technology-related problems, and report the problems to relevant IT units for investigation and resolution purposes, and to keep record of events and analyse and follow up the events until resolution of the reported problems.

(3) Bank implements a performance monitoring process so as to ensure that performance of information systems is continuously monitored, and contingencies are reported in a timely fashion. Performance monitoring process contains an early warning function ensuring that problems are identified and corrected before affecting the system performance, and provides information needed for a capacity plan in line with the planned business goals and objectives, and assists in preparation of workload forecasts.

(4) Bank manages and plans capacity in order to assure the existence and availability of an IT capacity capable of meeting and satisfying its existing and future business requirements set forth in IS strategy plan in accordance with the defined service levels and workload forecasts. Bank continuously maintains and updates its capacity plan, and manages performance of IS services in such manner to meet or exceed the performance targets of the agreed upon service levels, and ensures diagnosis and resolution of events and problems correlated to capacity.

(5) Bank is under obligation to employ methods capable of detecting that such repeated problems as fall in system performance, inadequate capacity and technical failures and breakdowns in days of intensive transactions of customers, like ends of month, aftermath of public holidays, and wage payment days are indeed following a certain pattern, and also to detect the root causes of these problems and ensure that they are resolved.

ARTICLE 27
Accessibility Management and Backup

(1) Bank is obligated to build redundant operation or standby mechanisms for critical hardware and systems in order to preclude a major part of system or banking activities from becoming non-functional or inoperative if and when any hardware or software component fails to function as expected from it. In deciding which hardware and systems are critical, accessibility requirements of IS services specified in article 28 and of service levels thereof and of information assets specified in article 6 are taken into consideration.

(2) Bank is liable to establish a backup mechanism fit and convenient to accessibility requirements of each data specified in article 6 for the sake of accessibility of data. In order for the system to be restorable from its backup, such components as operating system, application software and data which ensure operation of system are incorporated into the backup procedure. So as to make sure that backup mechanism is smoothly functioning, data available in backup environment are regularly tested through restoration processes. Backups are ensured to be protected by appropriate encryption techniques and physical security controls during transportation.

(3) Bank is further under obligation to build appropriate alternative communication channels against interruptions or failures that may be caused by network and communication infrastructure.

(4) Bank is also obliged to keep records reflecting the current situation as to which system, server and data backups are taken by which methods and in which frequency, and in which media, environments and positions these backups are kept.

(5) Immediately upon receipt of data requests from the Agency or juridical authorities handling an investigation or prosecution, bank is obligated to back up by taking a copy of all related data, or to keep the original data until such request is fulfilled. Bank is also required to deliver the requested data after converting the same to well-known formats in which the requesting authorities can easily examine data, or to provide the requesting authorities with applications or tools entailing them to examine the data, together with the requested data. Bank can by no means argue that the data storage time imposed by the applicable laws or regulations has expired and for this reason, the requested data are inaccessible, due to its own delay in processing the data requests submitted to it under this paragraph. Bank keeps and stores all copies or additional backups taken for the data requested from it under this paragraph for at least two years.

ARTICLE 28
Assurance of Continuity of Information Systems

(1) For the sake of continuity of IS services employed in performance of banking activities, an IS continuity management process and a Board of Directors-approved IS continuity plan are prepared and issued as a part of business continuity management and plan. An IS continuity management process supervisor is appointed and an IS Continuity Committee is built. IS Continuity Committee is comprised of representatives of bank's human resources, relevant business units, IS security function, and relevant IS units,

and if available in the organization chart, representatives of units or positions correlated to compliance and law, and is chaired by IS continuity management process supervisor. IS Continuity Committee is entrusted with the tasks of announcing a crisis event by taking into consideration all factors related to the events, and deciding to activate and start IS plan, and working in coordination with other rescue (recovery), continuity and response teams.

(2) IS continuity management process is essentially required to be based upon national or international standards or best practices as reference. Under this process, bank carries out the following activities in respect of IS continuity plan:

a) To establish an information systems continuity management process containing business impact analysis, risk assessment, risk management, monitoring and testing activities; and

b) To further develop the plan and determine the steps needed for rescue and recovery within the frame of business impact analysis conducted and business goals and objectives prioritized with participation of business units as well; and

c) To make sure that plan is feasible and duly maintained; and

ç) To ensure that plan is compliant with other plans such as response plans and capacity plan and with legislative requirements; and

d) To ensure that plan is reviewed and updated at least once a year in the light of lessons derived out of tests performed and findings determined as a result of audits and risk analysis works, or after changes affecting business processes or IS continuity; and

e) To handle legal issues arising out of emergencies and disasters, and conduct public relations and press communications; and

f) To make sure that relevant teams and employees are trained and awareness is increased under and by the plan.

(3) During the plan preparation process, through assessment of level of significance of information assets and data kept therein, within the frame of business impact analysis, acceptable interruption time and acceptable data losses are determined for each IS service, and recovery procedures allowing the services to become re-accessible are developed in line with said limits.

Bank also prepares procedures for restoration from secondary centre to primary centre upon completion of the event of disaster.

(4) Secondary centres are established under the plan. Data and system backups are ensured to be kept ready for use in secondary centre. Secondary centre is essentially required not to be exposed to same risks with primary centre geographically in terms of losses or damages that may be caused by such events as earthquake, fire, explosion, flood, inundation, landslide, power failures and communication line interruptions.

(5) Critical individuals in charge of conduct of plan and other personnel having responsibilities correlated to plan are liable to attend every year an IS continuity training with details and contents proportional to their functions and responsibilities, and are thus informed about their duties, functions and responsibilities relating to the plan.

(6) Even in disaster scenarios where primary systems are entirely deactivated, bank is essentially required to resume and restart its activities within maximum twenty-four hours. For the sake of efficiency and currency of plan, tests are performed at least once a year so as to put forth a real disaster scenario and to resume and continue banking activities through secondary centre. External service providers, if any, are also included in tests, and test results are reported to top management, and plan is updated according to these test results. The Agency is authorized to determine and issue additional procedures and principles for implementation of provisions of this paragraph.

(7) Validity of communication data of critical individuals in charge of conduct of plan and other personnel having responsibilities correlated to plan and external service providers, and accessibility of these individuals and their readiness to take office are tested at least twice a year through communication chain tests. Current copies of communication data and plan and relevant recovery or restoration procedures are required to be kept open for access at all times in a manner accessible by only individuals who need to know them, and these copies are ensured to be kept at the required locations and positions always.

(8) Bank makes sure that updates, patch uploads and configuration changes made in systems, servers, network devices and other IT components of primary centre are repeated likewise also in their backups kept in secondary centre, and performs integrity controls to guarantee that data and system backups copied to secondary centre are same as those kept in primary centre.

(9) Bank documents in such manner to reflect the current and recent situation the list of IS services, servers, systems, applications and data kept in secondary centre and the list of IS services, servers, systems, applications and data not transferred to secondary centre.

(10) Where certain services are outsourced for primary or secondary centre, or data are hosted in a data centre shared with other institutions, upon occurrence of a real disaster in the location of data centres or on regional basis, both the working environment in primary and secondary centres and the sources to be set aside by external service providers to bank are essentially required to be capable of guaranteeing the business continuity of bank.

SIXTH SECTION
Outsourcing of Services

ARTICLE 29
Management of Outsourcing Process

(1) Bank top management establishes and builds an adequate supervision mechanism allowing adequate assessment and management of risks that bank may be exposed due to outsourced services, and effective management of relations with external service provider. With regard to outsourcing, it is required to make sure:

a) that risks that may be caused by outsourced services are assessed and evaluated in all aspects; and

b) that due diligence and care is shown in selection of external service provider; and

c) that external service providers appointed as above and their service recipients and their communication data are written down and documented, together with expiration dates of services; and

ç) that accessibility, performance and quality of outsourced services, and whether the agreed service levels are complied with or not, and security breach events related to these services, and security controls of external service provider correlated to confidentiality, integrity and availability, and whether its operational and financial situation is fit to performance of its obligations or not, and its compliance with contractual terms and conditions are followed up and checked in regular intervals; and

d) that systems and processes covered by outsourcing are compliant with bank's own risk management, security and customer privacy policies; and

e) that where bank data are required to be transferred and disclosed to external service provider for outsourcing purposes, necessary actions are taken so as to make sure that the security-related principles and practices of external service provider are at the same level as those applied by bank; and

f) that external service provider must also be subject to the same audits as those applied if and when the outsourced activities are carried out within the bank organization, without any downscoping or downsizing; and

g) that outsourcing related details are regulated by taking into account the bank's business continuity plan, and all of the required actions are taken in connection therewith; and

ğ) that an exit strategy is determined so as to assure management of risks that may be exposed if and when outsourcing is terminated or interrupted beyond the initial plan; and

h) that the outsourced services may be transferred or assigned to subcontractors only with a prior consent and permission of the bank.

(2) Conditions, scope and all kinds of other definitions regarding outsourcing for services are documented in a written contract. Contract contains the following items at the minimum:

a) Definitions relating to service levels; and

b) Service termination conditions; and

c) Provisions regarding actions and measures required to be taken by external service provider in order to prevent hindrance or interruption of business continuity of bank; and

ç) Requirements in respect of sensitive issues under the bank's security policy, and provisions aiming to oblige external service provider to keep in strict confidence all information learned about bank and its customers, both during provision of services and after termination thereof; and

d) Provisions requiring external service provider to immediately report to bank all and any events such as security breaches or data leakages occurring in external service provider; and

e) Provisions as to ownership and intellectual property rights of products and services covered by contract; and

f) Clauses ensuring that contract provisions regarding obligations of external service provider are incorporated as binding articles into contracts to be signed with subcontractors as well; and

g) Provisions as to management of risks that may be exposed if and when outsourcing is terminated or interrupted beyond the initial plan; and

ğ) Provisions entailing delivery to bank or destruction of bank and customer data and information, as appropriate, upon termination of outsourced services; and

h) Provisions requiring that legislative provisions applicable on bank are made valid and applicable also for external service providers within the frame of outsourced services; and

ı) Clauses stating that external service providers are under obligation to disclose timely and accurately all kinds of information and documents requested by the Agency in respect of their activities, and to make ready for inspection all and any records kept in any kind of electronic, magnetic and similar other media and environments therefor, and to operate, run and make ready for inspection all systems and passwords needed for access to said records, and so as to make these records readable; and

i) Clauses verifying that bank and its independent auditor are authorized to request all kinds of information and documents from external service provider with regard to the outsourced services.

(3) Bank cannot acquire critical services by using outsourcing models applied within the frame of standard contracts where it is not possible to have the contractual terms and conditions and obligations specified in second paragraph implemented, nor can bank conduct its critical work flows by such types of outsourcing models.

(4) Bank checks whether such service providers as search engines and social media platforms from which it intends to purchase advertisement services regarding its banking services have already taken measures and actions for prevention of fake ads given in the name of bank or not, and cannot receive advertisement services from service providers failing to take the required appropriate measures and actions. Into contracts to be signed with

such service providers as search engines and social media platforms from which it purchases advertisement services, bank is obligated to incorporate clauses stating that in case of publication of fake ads, bank will be able to get the required information specific to the event for the sake of protection of customer. The provisions of this paragraph are valid and enforceable also for contracts to be signed with intermediary firms hired by bank for receipt of advertisement services hereunder.

(5) Bank makes the required organizational changes, and defines the required administrative procedures, and appoints a supervisor having adequate information and experiences for management of relations with external service provider, in order to keep under control all risks arising out of outsourcing for services, in tandem with the principles described in its security policy.

(6) Types of right of access granted to external service provider are specially assessed. For these physical or logical accesses, a risk assessment is performed, and additional controls are established depending on results of risk assessment. In risk assessment, type of access needed, value of data accessed, controls carried out by external service provider, and impacts of this access on security of bank information are taken into consideration.

(7) In outsourcing, bank is under obligation to take all measures required for security of its own confidential information and confidential information of its users. Authorizations to be granted to external service provider for access to system, access to data or to see the data are limited so as to cover only the information needed therefor. It is the responsibility of bank to ensure that external service provider also takes all measures for protection of its own confidential information and confidential information of its users.

(8) IS internal control and internal audit activities mentioned in this Regulation can in no event be outsourced, but will be performed by bank's own personnel.

(9) Bank's information systems may be entirely or partially made the subject of outsourcing, providing:

a) that bank reserves its decision making power and dominating role on such issues as management, content design, access, control, audit, updating, information/report receipt, etc., without any limitation thereto, over bank's information systems, in terms of banking activities and obligations required by banking laws and regulations; and

b) that bank is fully cognizant of all managerial details relating to information systems covered by outsourcing; and

c) that an authorization mechanism aiming to ensure that authorizations of access to bank's databases and data are managed absolutely in reliance upon permissions to be given by bank itself, whether it is critical information or not is established and employed, and that bank itself performs all internal control activities such as authorization for all of the applications being used by bank, and review of logs; and

ç) that all kinds of information and documents relating to accounts, records and transactions covered by outsourcing are kept under ownership of bank, without prejudice to intellectual property rights related to software.

(10) Maximum care is shown for production in Turkey of critical information systems and other products and services to be purchased for security purposes, or for location of R&D centres of their manufacturers in Turkey, and this is evaluated as an important criterion in outsourcing. These types of providers and manufacturers are essentially required to have response teams in Turkey. The Agency is authorized to determine and impose additional conditions about security products and other IT items and components to be used by banks.

(11) Bank may employ cloud computing services as outsourcing. Cloud service for primary or secondary systems may be received by a special cloud service model through hardware and software resources allocated to a single bank. Furthermore, outsourcing by collective cloud computing service model where only hardware and software resources allocated to institutions under the Agency supervision are physically shared, but separate resources are assigned specifically to each bank logically is subject to a prior permission of the Board. If deemed necessary, the Board is authorized to change institutions that may be included in collective cloud computing service model.

SEVENTH SECTION
Information Systems Internal Control and Internal Audit Activities

ARTICLE 30
Information Systems Internal Control Activities

(1) An IS internal control function is built and appointed in order to check compliance of IS management-related activities in bank and bank's external service providers, and processes supporting said activities, and IS controls

established therefor with the applicable laws and regulations and bank's internal policies, procedures and standards. An IS internal control supervisor is appointed, and IS internal control activities are carried out under responsibility of that supervisor. In addition, IS internal control function also performs the following activities and operations:

a) Sending reports and notifications to the related units and top management for taking actions and making up shortages detected as a result of controls; and

b) Sending notices to the related units and top management about process or systematic improvement suggestions understood to be needed as a result of controls; and

c) Upon demand, forming opinions about modifications and innovations planned in bank's products and processes or about bank's internal policies, procedures and process documents in relation therewith; and

ç) Attending the meetings of project and working groups, boards and committees related to critical processes within its fields of responsibility, and expressing suggestions aimed to minimize the risk in those meetings; and

d) Periodically reporting to top management, audit committee and internal control unit manager in respect of follow-up of risks arising out of IT management and outsourcing for services; and

e) Preparing IS internal control inspection plans every year in such manner to indicate the planned and scheduled inspections to be executed next year, and getting approval of bank audit committee therefor.

(2) IS internal control supervisor is essentially required to have a past professional experience of five years in total at the minimum in any one or more of IS internal control, IS audit, IT governance and controls or information security fields. Personnel to be assigned to IS internal control function are also required to have minimum knowledge and skills in the relevant fields as will be proven by their education status or by certificates taken by them.

(3) Periodical controls conducted as a part of IS internal control activities are recorded, and working papers of controls made as above are kept in the bank for at least three years.

ARTICLE 31
Information Systems Internal Audit Activities

(1) An IS internal audit function is built and appointed in order to provide assurance to board of directors about compliance of IS management-related activities in bank and bank's external service providers, and processes supporting said activities, and IS controls established therefor with the applicable laws and regulations and bank's internal policies, procedures and standards, and about effectiveness and efficiency of internal control and risk management activities correlated to information systems. An IS internal audit supervisor is appointed, and IS internal audit activities are carried out under responsibility of that supervisor.

(2) IS internal audit supervisor is essentially required to have a past professional experience of five years in total at the minimum in any one or more of IS internal control, IS audit, IT governance and controls or information security fields. Personnel to be assigned to IS internal audit function are also required to have minimum knowledge and skills in the relevant fields as will be proven by their education status or by certificates taken by them.

(3) Coverage of IS internal audits is required to be deep and detailed enough to contain critical IS services, processes and critical assets and to provide assurance thereabout. An IS audit plan comprised of IS areas auditable on yearly basis is prepared, and approval of bank audit committee is received therefor.

(4) Frequency and cycles of IS internal audits of bank are ensured to be proportional to criticality and riskiness of IS services, processes and assets. For IS internal audits to be performed so as to provide assurance as to full performance of all relevant provisions of this Regulation by bank, audit cycle is determined and arranged in such manner not to exceed two years.

(5) Audit guidelines and check lists are prepared in writing and documented for IS audits to be performed by IS internal audit function, and they are then regularly reviewed and updated in accordance with the current technologies. Working papers related to the audits conducted are kept in the bank for at least three years.

ARTICLE 32
Follow-up of Findings and Provision of Assurance

(1) Bank audit committee spares enough time for follow-up and handling of findings detected as a result of IS internal control, IS internal audit and other IS audit works, and directly reviews the critical issues determined by said works, and guides top management about the actions and measures required

to be taken therefor. Composition of members of bank audit committee is built so as to have adequate professional experience or know-how for appropriate assessment of IS internal control and IS internal audit reports and findings.

(2) Bank ensures that the findings detected as a result of IS internal control, IS internal audit and other IS audit works are duly followed up under an action plan. Findings for which a target completion date cannot be assigned in action plan for closure of findings, or the target completion date of which is exceeded, or excess time of which is extended for more than one year, or which are cancelled are regularly reported to audit committee, and these findings are handled as critical issues in audit committee.

(3) IS internal control and internal audit function makes suggestions about actions and measures that may be taken by the related audited unit for correction or remedy of its findings, or comes to mutual agreement about actions planned to be taken by the related audited unit in relation therewith. Final decision for findings which reach the closable status upon completion of implementation of suggestions and actions is given and pronounced as a result of examination thereof by IS internal control or IS internal audit function as the owner of finding.

(4) As a result of works performed by IS internal control and internal audit functions, it is essentially required to examine bank's IS controls and independently from the works conducted by independent audit firms, to make an assessment so as to find out all major and material control deficiencies in respect of said controls, and accordingly, to provide adequate assurance:

a) that bank's IS controls do not have any major material control deficiency which may hinder or prevent effectiveness, efficiency or compliance in the light of procedures and principles set down in this Regulation and in Second Part titled "Internal Control System" of ISEDES Regulation; and

b) as to non-existence of an event or situation which leads to a material misstatement in financial statements or materially affects the integrity, consistency, reliability, or if and when needed, confidentiality of data that are sensitive for bank, particularly financial data, and the continuity of activities related thereto, or non-existence of any fraud or collusion involved in by managers and other officers having critical duties and functions in internal control system; and

c) that if the resulting findings contain issues or events covered by subparagraphs (a) and (b), all of these issues or events are duly reported to bank audit committee and board of directors.

ARTICLE 33
Personnel Training and Resource Allocation

(1) For the sake of effective performance of IS internal control and IS internal audit activities, it is essentially required to employ personnel of adequate number and qualities, and to ensure that bank allocates adequate resources therefor. Personnel to be assigned for IS internal control and internal audit functions are ensured to take training and attend conferences and seminars in IS internal control, IS audit, IS governance and controls or information security fields for at least twenty hours a year and at least one hundred and twenty hours in three years.

(2) It is essential to make sure that IS internal control and IS internal audit activities are conducted in a coordinated manner in reliance upon mutual cooperation and information, and internal control and internal audit activities are planned in such manner to ensure that the systems, processes and areas having a high materiality level are assessed in a timely fashion and with priority, and the resources required for these activities are allocated fully.

THIRD PART
Electronic Banking Services

FIRST SECTION
Joint Provisions

ARTICLE 34
Identity Verification and Transaction Security

(1) Unless otherwise specified in this Regulation, for electronic banking services, also including transactions which do not lead to a financial result, such as display of customer data and information, banks are essentially required to apply on their customers an identity verification mechanism consisting of at least two factors independent from each other, and to take measures for confidentiality of identity verification data hosted therein during use of the aforesaid factors in identity verification process. These two factors are selected so as to belong to any two of different factor classes “known” or “owned” by customer or “having a biometrical characteristic”. Independence of factors means that the capture or acquisition of any one factors does not endanger the security of other factor. The factor owned by customer should essentially be specific to customer and not be imitated.

(2) In identity verification, if and when T.R. Identity Card is used together with card PIN or biometrical data, or electronic signature is used, the conditions of the preceding first paragraph are deemed to have been satisfied.

(3) On the basis of transactions executed through electronic banking channels, the Agency is authorized to define exceptions or additional security measures in respect of implementation of first paragraph, or to determine additional procedures and principles. For all kinds of banking transactions executed without use of a two-factor identity verification in contradiction with first paragraph hereof, the burden of proof lies with the bank for demonstrating that the related transactions are executed by customer.

(4) Factors to be used in identity verification mechanism to be applied on users are kept secure throughout the full process starting from production stages to the stage of delivery to user.

(5) Encryption keys to be used for identity verification purposes are presented for use by customer in such manner to cover methods minimizing the probability of retrieval or capture of these keys, and keeping them in strict confidence, and preventing their replacement and impairment.

(6) Identity verification mechanism to be applied on users is ensured to give information to the related user about unsuccessful identity verification attempts at the first moment the user enters the system. If unsuccessful attempts exceed a certain threshold, additional security measures are taken for access of customer, and if unsuccessful identity verification attempts are continued, access of the related user is prevented.

(7) To its customer who have uploaded and activated mobile banking application, bank may in no event send an OTP or verification code by SMS for login purposes or for verification of any transaction during sessions, nor may bank use the same as an identity verification factor. However, at the stages of first installation, activation and re-activation of mobile banking application or if the application becomes unusable, sending an OTP or verification code by SMS does not constitute a breach of provisions of this paragraph.

(8) Customers who have replaced their SIM card or have changed their electronic communication operator through number porting are determined by bank through establishment of the required integration with mobile communication operators resident in Turkey, before sending an OTP by SMS, and unless such changes are confirmed, the SIM card-based factor cannot be used as an identity verification factor in the course of provision of electronic banking services to the related customers for a period of 90 days following the date of change. In confirmation of said changes, for all types of transactions executed without use of two-factor identity verification mechanism, the burden of proof lies with bank for demonstrating that the related transactions are executed by customer.

(9) One time passwords to be used by customers for identity or transaction verification purposes are ensured to be of adequate length difficult to be estimated, and be produced randomly, variably and uniquely, and be valid for a particular period of time.

(10) Neither information which are used to determine the identity of customer and are given on documents serving as official identity document nor mother’s maiden name may be used for identity verification purposes at any stage during provision of electronic banking services. If and when bank wishes to use a security question as a customer-known factor for identity verification purposes, then and in this case, this security question should not be related to any one of information given on documents serving as official identity document, and its answer should be determined by the customer itself.

(11) If an identity verification factor is to be remotely associated with a customer for the first time, this association is made by secure methods and by using an at least two-factor identity verification mechanism in strict conformity to the preceding first paragraph. Cards covered by the Law on Bank Cards and Credit Cards no. 5464 dated 23/2/2006 and PIN belonging to payment tools covered by the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions no. 6493 dated 20/6/2013 cannot be used as "customer-known" identity verification factor as set forth in the preceding first paragraph, except for the transactions where card is used as the owned factor after the related electronic banking channel is activated and first password is received. If, after the related electronic banking channel is activated and first password is received, the password is required to be zeroed and changed due to forgetting or entry of wrong password, for remote determination of new password, the aforementioned PIN data may be used as the customer-known factor, providing that at least two-factor identity verification is effected in accordance with the preceding first paragraph.

(12) For transactions that may be executed via electronic banking channels, bank provides its customers with additional security measures such as access restrictions that are assumed and may be updated by customer, as well as daily transaction limits and secure recipients list. Security measures are essentially required to be identified, updated or changed only after identity verification affected in accordance with the preceding first paragraph. Bank may, however, determine security measures in addition to first paragraph for changes to be made in security measures within the frame of its own risk assessment.

(13) If the reverse of any transaction offered via electronic banking channels is feasible and is equally or less risky than the original transaction, bank ensures that these transactions being reverse to the original transaction are also affected and performed through the same electronic channel.

(14) It should be verifiable that all kinds of software or mobile applications offered by bank to its customers for use in electronic banking services are sourced or originating out of the related bank. Bank is further obligated to make sure that these software or mobile applications do not contain any code threatening customer security, and to provide the customer for its use with all patches and updates needed to close and remedy said security vulnerabilities.

(15) Bank takes actions and measures so as to make the critical data used by banking applications over mobile devices, such as smart phones, employed in transmission of several identity verification factors to bank inaccessible by

other applications or transactions run on the same mobile device. Bank is further under obligation to make the critical data on said mobile devices inaccessible by unauthorized persons if and when mobile devices are lost or stolen, and to establish controls fit to the current technology with a view to reducing risks that may arise out of capture of mobile devices, or impairment of their reliability, or breakage or replacement of operating system software.

ARTICLE 35
Non-Repudiation and Responsibility Assignment

(1) Bank uses techniques making non-repudiation and responsibility assignment possible for both bank and customer in transactions executed as a part of electronic banking services offered by it. Logs created by the techniques used are ensured to be capable of giving reliable evidences and of assignment of responsibilities.

ARTICLE 36
Follow-up of Transactions

(1) Bank establishes and uses transaction follow-up mechanisms aimed to detect and prevent extraordinary or fraudulent transactions or transactions with fraud risk executed under and as a part of electronic banking services. If and when it is appropriate under the transaction follow-up mechanism, the following risk components are followed up at the minimum:

a) Known fraud methods in respect of transactions leading to financial results; and

b) Whether each banking transaction executed as above demonstrates an abnormal payment, fund transfer or behaviour pattern or not, in the light of its amount, and customer's location data according to said amounts; and

c) List of identity verification factors lost, stolen or captured by unauthorized persons; and

ç) Signs indicating the probability of infection of malicious software programs in respect of each identity verification session.

(2) Bank evaluates and assesses risky transactions by filtering them, and follows up the customers caught in these filters more closely. If risky transactions are detected, bank makes sure that customers are warned by appropriate methods such as telephone or short message service as soon as possible.

ARTICLE 37
Informing Customers

(1) Customers wishing to make use of electronic banking services offered by bank are clearly kept informed about conditions, risks and exceptional situations related to services. Security principles adopted by bank in order to mitigate the impact of risks pertaining to electronic banking services, and methods required to be used so as to be protected from these risks are presented to the attention of customers. All kinds of information and explanations aiming to keep customers informed as stipulated in this Regulation are at all times kept open to customer's access both in the bank's own internet site and in the internet site through which internet banking services are offered by bank, and techniques are used to demonstrate that these sites accessed as above belong to bank. Information and explanations are ensured to be open, clear and understandable, and are placed at an attention-grabbing place in the internet site, and guidance and systematic restrictions are applied in order to guarantee that customers read them at least once before starting to use the related electronic banking services. Also for the important security warnings and announcements required to be presented to the attention of customers after they start to make use of the services, techniques are used so as to make sure that these warnings and announcements are read by customers.

(2) Under the first paragraph, either bank's own internet site or the internet site through which internet banking services are offered by bank contains:

a) information about bank's identity, trade name, address of head offices and legal status, and communication information of the Banking Regulation and Supervision Agency which is responsible for audit of banks; and

b) risks of use of electronic banking services, and methods required to be used by customers for protection from these risks, and directive security guidelines needed for increase of customer awareness, and responsibilities and rights of customers wishing to make use of these services; and

c) electronic banking services offered by bank, and days and hours when these services and banking transactions that may be executed under these services are open for access, and other conditions related to services; and

ç) notices and announcements aiming to inform customers in advance about scheduled maintenance and replacement works requiring interruption of longer than two hours in electronic banking services; and

d) instructions and information about the actions required to be taken by customers if and when they face any problem or any event of fraud in the course of services.

(3) Mechanisms to be used by customers for follow-up and reporting of their probable problems and complaints in respect of electronic banking services are established. In menus seen by customers in complaint units or call centres to be built, the act of reporting of fraud events in respect of the related electronic banking services is required to be presented to attention of customer in the main menu and in first orders, and necessary actions are required to be taken for response and satisfaction of notifications delivered to bank as soon as possible.

(4) In electronic banking services provided by bank, it is ensured that controls are built and established so as to minimize the probability of wrong transaction of customers, and that all kinds of commissions, fees and other moneys required to be paid by customers for the transactions initiated therein are clearly notified to the customer at the moment of transaction, and that the transactions are executed only if and when these expenses are approved by customer.

(5) Bank cannot open its internet banking and mobile banking services for use by customer without a demand of customer. If customer closes its access to any electronic banking service, that service cannot be re-opened for use without a new demand of customer.

(6) In its marketing activities, advertisements or publications, bank refrains from using statements or expressions arguing or giving an impression that any electronic banking service offered to its customers are absolutely and definitely secure or are entirely free from any security risks whatsoever they are.

(7) In the event that information required to be given about electronic banking services offered by bank pursuant to and under this Regulation remains insufficient in terms of information possibilities due to reasons attributable to the platform used for services or the device used by customer for receipt of services, the required guidance is given so as to enable the customer to reach same information through different channels.

(8) All kinds of information, such as account extracts, advice notes and account statements, containing critical or confidential data to be transmitted by bank to its customers via electronic media are essentially required to be

sent via channels used for provision of electronic banking services. Bank is under obligation to give the required guidance to its customers for use of electronic distribution channels in provision or disclosure of such information.

SECOND SECTION
Internet Banking

ARTICLE 38
Identity Verification and Transaction Security in Internet Banking

(1) Identity verification transaction to be executed in internet banking channel according to first paragraph of article 34 is required to be affected online in the bank, not offline at the locality, and the customer-known factor should not be sent automatically by being remembered by mobile banking application or internet browser, or through linking of this factor to other local identity verification methods. Customer-known factor is required to be entered by customer, and this factor is verified online in bank, not at the locality, without prejudice to provisions of second paragraph of Article 34.

(2) In the course of an identity verification transaction in internet banking channel, after a two-factor identity verification factor is entered by customer or sent to bank, and before an internet banking session is opened, it is ensured that a welcome message or picture predetermined by customer with a two-factor identity verification factor according to first paragraph of Article 34 is shown to customer.

(3) A one-time verification code is generated for signature by a private key assigned to customer for identity verification transaction to be executed in internet banking channel according to first paragraph of Article 34. It is ensured that information cannot be obtained through verification code about any one of identity verification factors mentioned in first paragraph of Article 34, and that other valid verification codes cannot be derived out of a known verification code, and that verification codes cannot be imitated. It is also ensured that verification codes developed for transactions leading to financial results are specific according to customer-approved amount and recipient information, and that in case of any change in information as to amount or recipient of funds, the related verification code generated according to such information also becomes invalid. In such transactions as fund transfer where collective transactions are permitted to be executed in bulk for several recipients in respect of corporate internet banking customers, the verification code to be generated is required to be specific for the relevant bulk transaction total amount and recipients. Where it is not possible to sign a verification code

by using a private key assigned to customer, a verification code may be transmitted to customer by SMS, without prejudice to proviso of seventh paragraph of Article 34.

(4) At each stage of verification process, also including the generation, transmission and use of verification code for customer-executed transactions leading to financial results in internet banking, the required actions and measures are ensured to be taken for the sake of confidentiality, reliability and integrity of information, such as amount and recipient information, demonstrated to customer and presented to its approval, and against the risk of guidance of data communication to unauthorized individuals during internet banking session.

(5) In case of an error in generation of verification code or in case of failure in generation of it, the person making the identity verification attempt takes actions and measures so as to ensure that it cannot be understood from which identity verification factor the error arises.

THIRD SECTION
Mobile Banking

ARTICLE 39
Identity Verification and Transaction Security in Mobile Banking

(1) If and when an application PIN identified to mobile banking application is used to have access to a customer-specific encryption key, and a unique information related to customer is verified online in the bank through this encryption key, then and in this case, two-factor identity verification described in first paragraph of Article 34 is deemed to have been affected. Similarly, if and when a biometrical identity verification component belonging to customer is used in mobile banking application to reach an encryption key specific to customer, and a unique information related to customer is verified online in the bank through this encryption key, then and in this case, two-factor identity verification described in first paragraph of Article 34 is again deemed to have been affected.

(2) Passwords, PINs or biometrical data which are not under control of mobile banking application, but under control of device manufacturer cannot be used as customer-known factors or factors with biometrical characteristics as mentioned in first paragraph of Article 34.

(3) Providing that device loaded with mobile banking application and/or mobile banking application itself is used as an identity verification factor linked to and owned by customer, in the event that customer wishes to display customer and account data and information only through mobile banking application or to transfer money or make payment to a predefined secure recipients list, an identity verification made by a single factor without need to any additional identity verification factor is not considered and treated as a breach of first paragraph of Article 34. If and when customer logs in for the first time in order to display customer and account information specified in this paragraph, or more than 90 days have passed after the last session logged in by customer through identity verification by two factors according to first paragraph of Article 34, then and in this case, customer is essentially required to be subject to a two-factor identity verification mechanism.

FOURTH SECTION
Telephone Banking

ARTICLE 40
Identity Verification, Transaction Security and Service Quality in Telephone Banking

(1) As long as the customer does not affect identity verification in accordance with first paragraph of Article 34, the officer welcoming customer for telephone banking services should not see customer-related information or customer-related transaction menu should not be active. In identity verification to be applied for execution of financial transactions between customer's own accounts and non-financial transactions, PIN data may be used as customer-known factor. In case of notification of a risky transaction such as loss, theft and fraud, without an identity verification of customers linked to officer, the officer should have access only to certain customer data and information needed to be known, and all required security measures are also taken therefor. Without a telephone call or after termination of telephone call, no customer-related transactions can be executed other than notification of a risky transaction such as loss, theft and fraud.

(2) If and when customer wishes to change its identity verification or telephone information used in any one of electronic banking channels via telephone banking, then and in this case, such change is ensured to be executed via automatic systems without any interference or access of an officer.

(3) In the course of identity verification during provision of telephone banking services, customer-known identity verification factors and such other

factors as one time password or transaction verification code are ensured to be entered via automatic systems without any interference or access of an officer.

(4) Where the customer is required to be called through its telephone number registered in bank, before the telephone call, controls are run so as to make sure that the telephone is not directed to another number.

(5) For voice records in respect of transactions executed by customer during provision of telephone banking services, the provisions of this Regulation pertaining to logs are applied. The voice records taken as above are required to be of a quality and description to ensure that reliable evidences are obtained and responsibilities are assigned as required.

(6) Bank is under obligation to ensure that its employees such as customer representatives and call centre officers assigned for provision of telephone banking services to customers take periodical trainings about social engineering attacks and other known fraud methods, and to perform activities aiming to increase security awareness of aforesaid employees.

(7) Bank satisfies and meets the following criteria at the minimum for the sake of enhancement of telephone banking service quality:

a) Announcement time of main and sub-menus of interactive voice response system, also including advertisements, notifications and public disclosures, is ensured not to exceed sixty seconds each; and

b) In voice guidance system, customer should be given a time of ten seconds twice following the announcement so as to start telling its intended transaction, and thereafter, any customer failing to execute its transaction should be transferred back to main menu; and

c) Main menu or sub-menus offer the option of being linked to call centre officer or customer representative; and

ç) Such applications as limitation of length of conversation of call centre officer or customer representative with customer for the sake of achievement of call answering goals should not be used.

FIFTH SECTION
Open Banking Services

ARTICLE 41

Identity Verification and Transaction Security in Open Banking Services

(1) Providing that communication between customer or any party acting for and on behalf of customer on one side and bank on the other side is in the form of end-to-end secure communication during use of open banking services, and bank applies additional compensating controls, and additional restrictions are imposed on resources that the customer may be linked to, identity verification made by a single factor is not considered and treated as a breach of first paragraph of Article 34.

(2) The Board is authorized to determine services that can be provided through open banking services, and procedures and principles applicable on such services.

SIXTH SECTION
ATM Banking

ARTICLE 42
Identity Verification and Transaction Security in ATMs

(1) Bank is under obligation to take the required measures against known crime tools and techniques in order to prevent card cloning or frauds on ATM devices. Bank takes the following actions and measures at the minimum:

a) Techniques making it difficult for foreign devices such as false faceplate, false keyboard, card jamming apparatuses, card cloning apparatuses, banknote jamming apparatuses and mobile camera which can be installed inside card reader, at money entry and exit points or other units of ATM to be fitted to ATM, and for the existing ATM equipments to be removed from ATM, and preventive or detective controls are employed therefor; and

b) In periods to be determined as a result of risk analyses, ATM devices are physically controlled against existence of foreign objects. The related control periods are shortened for ATMs where the probability of fixation of card cloning and card fraud devices is high.

(2) If and when it is detected that any card cloning or fraud-purpose object is fitted to ATM, or ATM device is tampered, or solutions aiming to prevent card cloning and fraudulent acts generate an alarm, and these solutions do not function, then and in this case, it is ensured that ATM can be centrally deactivated for security purposes, and that it cannot again be put into service

without a physical control or without an assurance as to non-existence of any problem in reliance upon examination of camera views.

(3) All kinds of passwords given as defaults on ATM devices are changed in such manner not to be easily estimated or predicted, with a view to precluding malicious persons knowing these default passwords from managing or guiding ATM device.

(4) Required actions and measures are taken to prevent unauthorized access to ATM devices and uploading of malicious programs on ATM devices by malicious persons, and integrity of applications and critical services and data relating to applications is periodically verified. Updates and patches needed for correction and remedy of security vulnerabilities are uploaded on ATM devices automatically or in regular periods. Operating system running on ATM devices is ensured to be a stable and secure operating system, fit to current technologies, calibrated to work with the minimum required powers and privileges, and compacted through uploading of the required updates and patches. Bank takes actions and measures to prevent operation on ATM devices of applications and codes the source and integrity of which cannot be approved or proven.

(5) All points of entry which allow connection of another electronic device to ATMs by unauthorized persons in any way whatsoever are closed for access, and required additional security measures are applied to prevent unauthorized linking of other devices to the network connection between ATM device and bank.

(6) Communication network used for transactions executed via ATM devices is ensured to be capable of assuring data security, confidentiality and integrity. Confidentiality and integrity of all kinds of data stored, kept, transmitted and processed over ATM devices are protected by appropriate methods. Critical information used for identity verification purposes, such as PIN information, fingerprint information and card information are ensured to be kept confidential and in integrity starting from the moment they are digitalized and entered into the system.

(7) Bank is engaged in works creating awareness in its customers about secure use of ATM devices.

(8) If and when transactions legally requiring submission of identity if executed in bank branches are intended and wished to be executed via ATM devices, identity verification is applied in accordance with provisions of first paragraph of Article 34.

(9) Bank places a security camera in locations of ATM devices at an appropriate angle so that the camera cannot see the customer's keyboard movements. Security camera records are kept for at least six months. Videos in camera records are required to have evidential value, and video quality is required to entail determination of appearance and description of customer and his immediate circle on ATM device. Camera hours are ensured to be current and correct, and such parameters as reference number and advice note number of transactions executed on ATM device are ensured to be compliant with timing data. A structure capable of detecting fall of video quality of camera, suspension of recording of videos, closure or deactivation of camera lens by an external effect or for any reason whatsoever, and ensuring that the required actions are taken is established and installed.

(10) In case of existence of a security camera infrastructure covering also ATM device within its view area and meeting the conditions set down in ninth paragraph hereinabove, there is no need to install a separate security camera specifically for ATM device. The condition of installation of security camera for ATM devices located within activity zones of public security and intelligence authorities is fulfilled only with a prior permission of the related public security and intelligence authorities.

FOURTH PART
Miscellaneous and Final Provisions

FIRST SECTION
Miscellaneous Provisions

ARTICLE 43
Remote Identification and Trust in Third Parties

(1) Without prejudice to its obligations arising out of the Law on Prevention of Laundering Proceeds of Crime no. 5549 dated 11/10/2006 and its regulations, bank may, with a view to determining identity of customer or any person acting for and on behalf of customer, employ remote identification methods or receive service through open banking services from another bank which has already determined identity of customer or any person acting for and on behalf of customer. The Board is authorized to set down and determine the procedures and principles pertaining to implementation of this paragraph.

ARTICLE 44
Areas and Periods Regarding Professional Experience

(1) The Agency's professional staff members assigned in the department in charge of conducting IS on-site audits in the related institutions in the name of the Agency in accordance with the Regulation on Organization of Banking Regulation and Supervision Agency, put into force by a Decree of the Council of Ministers, no. 2014/5885, dated 2/1/2014 are deemed to have worked in the areas of professional experience mentioned in this Regulation, and the periods of work of such professional staff members in the related department are accepted as periods of work in areas regarding professional experience.

ARTICLE 45
Exceptional Provision

(1) About committees, units, departments and supervisors to be created or appointed under this Regulation, the Agency is authorized to define an exception on the basis of such criteria as banks' scale, dependence on information systems, number of personnel, and services outsourced.

SECOND SECTION
Final Provisions

ARTICLE 46
Effective Date

Article revised and amended by the Regulation Amending the Regulation on Information Systems and Electronic Banking Services of Banks (Official Gazette 20.06.2020 / 31161) article 1

(1) Article 13, Article 29, thirteenth paragraph and fifteenth paragraph of Article 34, eighth paragraph of Article 37, Article 40 and Article 42 of this Regulation shall become effective on 1/7/2020, while other provisions shall become effective on 1/1/2021.

ARTICLE 47
Enforcement and Execution

(1) The provisions of this Regulation will be executed and enforced by the President of the Banking Regulation and Supervision Agency.