By the Banking Regulation and Supervision Agency:

COMMUNIQUÉ ON PRINCIPLES TO BE CONSIDERED IN INFORMATION SYSTEMS MANAGEMENT IN BANKS[1]

(Published in the Official Gazette dated September 14, 2007, Nr. 26643.)

SECTION ONE
Initial Provisions

Objective and Scope

ARTICLE-1 (1) The purpose of this Regulation is to lay down the minimum principles and procedures to be considered in information systems management which banks use in performing their activities.

Basis

ARTICLE-2 (1) This Communiqué has been prepared on the basis of the Articles 11(5) and 16(3) of the Regulation on Internal Systems of Banks published in the Official Gazette dated November 1, 2006 and Nr. 26333 and the Article 93 of the Banking Law dated October 19, 2005 and Nr. 5411.

Definitions and Abbreviations

ARTICLE-3 (1) The following terms used in this Regulation shall have the meanings expressly designated to them below:

a) **(Amended: OG-01/06/2010-27598)** Emergency and unexpected situation plan: Emergency and unexpected situation plan defined in Article 3 of Regulation on Internal Systems,

b) ATM: Electronic transaction machines enabling all or part of banking transactions as well as automated teller transaction,

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

[1] Amended pursuant to the "Communiqué on Making Amendments to the Communiqué on Principles to be Considered in Information Systems Management in Banks" published in the Official Gazette dated January 24, 2009 and Nr. 27120

ç) Information systems management: Activities on establishing appropriate information systems environment, using information systems resources productively, controlling and monitoring the risks to derive from the usage of information systems and taking necessary systematic and administrative measures for this purpose, in order to effect activities conducted and services offered by banks in an efficient, reliable and uninterrupted way; to fulfill the obligations derived from legislation; to provide integrity, consistency, trustworthiness, and secrecy of information procured from accounting and financial reporting system and that information to be acquirable in time,

d) **(Amended: OG-01/06/2010-27598)** Information systems continuity plan: Information systems continuity plan defined in Article 3 of Regulation on Internal Systems,

e) BSDHY: Regulation on Information Systems Audit to be performed in Banks by External Audit Institutions published in the Official Gazette dated May 16, 2006 and Nr. 26170,

f) **(Amended: OG-01/06/2010-27598)** Primary center: The structure in which primary systems defined in Article 3 of Regulation on Internal Systems are established,

g) **(Amended: OG-01/06/2010-27598)** Primary systems: Primary systems defined in Article 3 of Regulation on Internal Systems,

ğ) Audit trail: Record that enables a financial or operational transaction to be trailed from the beginning until the end,

h) Electronic signature: Electronic signature defined in the Electronic Signature Law dated January 15, 2004 and Nr. 5070,

ı) Security wall: software or hardware based solutions which enable controlled access among webs having different security sensitivity levels,

i) Internal Systems Regulation: Regulation on Internal Systems published in the Official Gazette dated November 1, 2006 and Nr. 26333,

j) Internet banking: Banking service distribution canal that enables customers to reach via internet the services offered by the bank and to perform the transactions they wish to conduct,

k) Code Transaction Verification: The code composed of series of alphabetic and/or numerical characters for a transaction that a person wishes to perform who introduces oneself to the system through one of the identity validation methods and which is directed to the identity introduced to the system and created for single use only asking if he/she approves the transaction or not,

l) Law: Banking Law dated October 19, 2005 and Nr. 5411,

m) Identity validation: Mechanism that reassures that the identity disclosed actually belongs to the person disclosing,

n) **(Amended: OG-01/06/2010-27598)** Secondary center: The structure in which secondary systems defined in Article 3 of Regulation on Internal Systems are established in a way to be available for use and which enables the personnel to operate in an uninterrupted manner and in a way not to hold the same risks as the primary center,

o) **(Amended: OG-01/06/2010-27598)** Secondary systems: Secondary systems defined in Article 3 of Regulation on Internal Systems,

ö) Password: Series of secret alphabetical and/or numerical characters that is used in identity validation and that is not required to be changed,

p) **(Amended: OG-01/06/2010-27598)** Work impact analysis: Work impact analysis defined in Article 3 of Regulation on Internal Systems,

r) Leak test: Attacks realized in order to determined and correct security deficits of the system before being abused,

s) Public key cryptography: Encryption key used in public key cryptography, open to everyone’s access and usage, mathematically connected with public key cryptography and used in controlling the signature signed with public key cryptography, decrypting or

encrypting its location in a way public key cryptography can decrypt,

ş) **(Amended: OG-01/06/2010-27598)** Interruption: Interruption defined in Article 3 of Regulation on Internal Systems,

t) Encryption secret key: Key which is used in signing, encrypting and decrypting the data encrypted by equivalent public key cryptography and which should be known and used by the owner,

u) Single use password: Series of alphabetical and/or numerical characters created randomly to be used in identity validation,

ü) Senior management: Senior management defined in the Article 3 of the Regulation on Internal Systems,

v) Top-level management: Top-level management defined in the Article 3 of the Regulation on Internal Systems,

y) Patching: Deficits determined in programs or program appendage prepared in order to correct a defective function in the content of the program,

z) Authorization database: Structure in which customer of user access rights or information on authorization are kept.

Importance of information systems management in banks

ARTICLE-4 (1) The bank treats information systems management as part of corporate management practices. Strategies relating to information systems are adjusted to the business targets for the bank to carry out its operations in a stable, competitive and improving line, factors concerning information management are positioned in the appropriate place within the administrative hierarchy and necessary financing and human resource is assigned for accurate management of information systems.

(2) The Bank establishes policies, procedures and processes concerning information systems management. Procedures and processes are reviewed and renewed, if necessary, on a regular basis in accordance with the changes in the line of business or technologic developments.

3) Efficiency of the management established on information systems is provided by the contribution of studies to be performed within the scope of risk management, internal control system and internal audit.

SECTION TWO

Risk Management on Information Systems and Establishment of Internal Controls

PART ONE

Risk Management on Information Systems

Information Systems risk management

ARTICLE 5 — (1) The bank takes necessary measures in order to measure, monitor, control and report the risks derived from information technologies usage in banking activities. Management of risks concerning information systems is treated as a significant component of information systems management. Among factors that may be considered as the main resource of the risks derived from the usage of information technologies in banking activities, those listed below are taken into consideration by the bank and included in the assessment:

a) Negative results of failing to follow the developments in information technologies in a competitive environment owing to the rapid developments in this field as well as difficulties in following these developments,

b) Possibility of information systems to lead up to errors different than familiar ones and frauds,

c) Procurement of support service which became widespread as the use of information systems in banking activities increased, hence dependence to support service institutions in operations arose,

ç) Business continuity of the bank became dependent mainly on the operability of information systems,

d) Providing the safety of transactions realized and data recorded, transmitted and processed through information systems, keeping record relating to customer identification, incontestability and data trails became difficult.

(2) The bank risk reviews management policies and processes depending on usage of information technologies and renews them so as to include the management of risks which may derive from this. As well as the risk derived from information technologies are considered within the scope of operational risk, due to the possibility of these risks may be a multiplier of other risks derived from banking activities, an integrated risk management approach including the risks derived from information technologies is adopted for all banking activities, data acquired from studies relating to follow-up and surveillance of information technologies is furnished to become a part of integrated risk management framework of the bank.

(3) The bank, having considered the planned changes, repeats the risk analysis on information systems and prepares the procedures how the risk analysis shall be performed in periods it shall assign or before significant changes to occur in information systems.

(4) Requirements of policies and procedures improved with a view to management of risks concerning information systems are positioned within the organizational and administrative structure of the bank so as to enable them to function actually, surveillance and follow-up on the operability of them are carried out.

(5) Risk management principles derived from special qualifications of information systems included in the Articles 6 to 9 of this Communiqué are taken into consideration in regulation studies of policies, procedures and processes concerning risk management in a way to include

the risks derived from the usage of information technologies. The said principles indicate the actions to be taken within the scope of top-level management surveillance, security controls and legal and reputation risk management. According to the risk profile, operational structure, corporate management culture of the bank and the framework defined upon the related legislation, it is essential that the bank should develop risk management processes and evaluate the risks derived from information technologies accordingly.

Management surveillance

ARTICLE 6 — (1) Top-management of the bank carries out an efficient surveillance in order to manage the risks derived from the usage of information systems. For this purpose, a comprehensive process is prepared by top-management concerning the management of risks derived from usage of information systems which were evaluated and of which appropriateness approved by top-management. This process consists of clear definition of responsibilities and establishing policies relating to management of risks and establishing and monitoring controls.

(2) It is the responsibility of the Board to establish efficient and sufficient internal controls on information systems.

(3) Projects on usage of new information system elements which will have important impacts on risk profile and strategy of the banks are reviewed by the top-management of the bank. Top-management does not approve the studies unless it makes sure the bank has the necessary expertise level to manage the risks these new projects relating to information systems elements shall bring. It is principal that senior management and personnel expertise shall be proportional with the technical detail and complexity that practices relating to the project as well as the substructure supporting this require, without considering the projects are carried out through internal resources of the bank or by outsourcing. Administrative role and responsibilities to be established in order to support this structure are determined clearly.

(4) Senior management of the bank displays the necessary determination in bringing the security measures relating to information systems to the suitable level and allocates the necessary resource relating to the activities to be carried out for this purpose. Senior management establishes the mechanisms that will ensure the activities below are carried out, which are:

a) Reviewing information security policies and all responsibilities periodically and putting them through approval mechanism,

b) Evaluating treats against information resources periodically,

c) Monitoring situations relating to information security violation and evaluating them periodically,

ç) Supporting studies to increase awareness relating to information security.

(5) Information security policy of the bank shall be approved by the administrative board and be supervised by the applied top-level management.

Establishment and management of security control process

ARTICLE 7 — (1) Top-level management of the bank puts security control process into evaluation and certifies its appropriateness so as to ensure the security risks derived from information systems are managed adequately within the scope of information security policy. Top-level management of the bank carries out the supervision studies of developing and updating regularly the control infrastructure relating to the measures that will ensure secrecy, integrity and accessibility of information systems and data to be processed, transferred, stored and held in reserve.

(2) Through security control process and information security policy, responsibilities are assigned to the persons in a clearly defined way. Clear administrative responsibilities relating to establishing, maintaining and managing security control processes accordingly are determined.

(3) Controls that shall be applied in order to establish information security involves the following elements as a minimum, which are:

a) In accordance with establishing the necessary controls and structures in respect of information systems and the security of the data they include; a process is established including making risk assessment, establishing and applying information security policy, implementing information security tests, monitoring and reporting the transactions and updating the controls and structures that has been built according to the technologic developments.

b) The bank ensures its personnel to raise awareness in respect of security, security policy of the bank is transferred to them and written commitments on adaptation are received.

c) Information systems and data to be processed, transferred, stored and held in reserve are classified according to their security sensitivity levels and security controls at appropriate level are established for each classification.

ç) Processes are established that shall ensure the reliability and consistency of information systems to be analyzed on a regular basis. Accordingly, leak tests are performed regularly to independent teams that have no executive assignment in respect of executing the requirements of the provisions relating to security. Current developments in security field and new deficits are monitored, necessary software updates are made and the necessary patching is implemented.

d) The bank establishes the necessary web control security systems against the treats that may emerge from external webs in cases of communication with those webs excluding its corporate web.

e) The bank uses one or more than one security wall that has been configured as required and is monitored continuously, in order to control the accesses to internal web from external web, in addition, to ensure controlled access by separating substructures of internal web that has different security sensitivity apart.

f) An information systems security responsible is assigned having the sufficient technical information and experience and who is responsible for implementing and monitoring the provisions on information systems security, repotting to information systems manager about the risks on information systems security as well as on managing these risks.

Management of support service procurement process on information systems

ARTICLE 8 — (1) Concerning the support service to be procured within the scope of information systems, top-management of the bank establishes a sufficient surveillance mechanism that will enable the risks to arise in respect of the bank in performing the said service through procurement of support service are evaluated, managed and the relations with support service institution are carried out effectively. By the surveillance mechanisms to be established, it is ensured, as a minimum, that;

a) Evaluating the risks that procurement of support service concerning information systems infrastructure shall bear in all its parts,

b) Paying the necessary attention in selecting support service institution,

c) Ensuring all system and processes within the scope of procurement of support service are appropriate to risk management, security and customer confidentiality policies of the bank,

ç) In cases when data of the bank is required to be transferred to the support service institution within the scope of support service, ensuring the principles and practices of support service institution on security are, at least, at the level the bank implements.

d) In case the activities within the scope of procurement of support services are carried out under the structure of bank, putting those activities through the same supervisions depending on whichever supervisions they are foreseen to be subject to and without narrowing any kind of scope; and executing additional supervision, in case required due to the fact that the activity has been carried out through procurement of support service,

e) Regulating the subjects concerning procurement of support services having regard to the bank business continuity plan and taking necessary measures and clarifying the responsibilities of support service institution within this scope via contract.

(2) **(Amended: OG-01/06/2010-27598)** An exit strategy is adopted appropriate to the management of risks concerning the cases of the termination or interruption of procurement of support service other than planned.

(3) Condition, scope and any definitions relating to procurement of support service is bounded by contract to be signed by the related support service institution. The contract, as a minimum, includes;

a) Definitions relating to service levels,

b) Termination conditions of the service,

c) Provisions relating to the measures that support service institution should take so as to prevent the business continuity plan belonging to the bank are interrupted,

ç) Requirements concerning the subjects that bear sensitivity within the scope of security policy of the bank,

d) Provisions regulating ownership of the product to be produced within the scope of the contract having regard to intellectual properly rights,

e) Provisions that ensure the provisions that are binding for support service institutions upon the contract to appear as binding agents also in the contracts to be drawn with subcontractor institutions,

f) **(Amended: OG-01/06/2010-27598)** Provisions on management of risks to derive from termination or interruption of procurement of support service other than planned,

g) Provisions that will ensure the legal provisions which the bank is subject to are applicable for the support service institutions as well within the scope of the service being procured.

ğ) **(Additional: OG-01/06/2010-27598)** In case of procurement of support services concerning primary or secondary systems, provisions that will ensure any change that should be made to primary or secondary systems of banks upon the direction of the Board or the Agency, to be fulfilled by support service company within the instruction period pursuant to the service being procured,

(4) The bank, in accordance with the principles the security policy defined, makes the necessary organizational changes in order to control the risks derived from procurement of support services, defines administrative procedures and integrates the measures to be taken accordingly with daily transactions and systems of all the related departments, assigns a responsible having sufficient information and experience to carry out the relations with the support service institution concerning the support service being procured.

(5) Access right types given to support service institutions are evaluated privately. Risk assessment is carried out for these accesses that can be physical or logical; accordingly, additional controls are established if necessary. Access type needed while performing risk assessment, value of the data being accessed, controls being carried out by support service institution and the impacts of this access on the security of bank information are taken into consideration.

(6) Top-management of the bank, concerning the services to be carried out through procurement of support service, monitors closely accessibility, performance, quality of the service, security violations realized within the scope of this service and security controls, financial conditions and appropriateness to the contract of the support service institution.

(7) In procurement of support service relating to information systems, the provisions included in this article are considered as additional provisions, on condition that the provisions determined in the Regulation on Banks' Procurement of Support Services and Authorization of Such Service Providers published in the Official Gazette dated November 1, 2006 and Nr. 26333 are exactly valid.

Identity validation

ARTICLE 9 — (1) An appropriate identity validation mechanism is established for the transactions performed via information systems. Which identity validation mechanism is going to be used is decided according to the risk assessment result to be carried out by top-management. Risk assessment is performed having regard to the type of transactions planned to be realized through information systems (such as type, quality, if any, size of financial and non-financial effects) sensitivity level of the data subject to transaction and ease of use of identity validation technique.

(2) Identity validation mechanism to be implemented is established so as to contain the whole process from customers and personnel being included in information systems to completing their transactions and leaving the system. Necessary measures are taken so as to ensure the identity validation information is accurate from the beginning of the session until the end.

(3) Necessary measures are taken so as to ensure the security of database in which identity validation data which is used for access to information systems is kept. Measures to be taken for this purpose, as a minimum, include preserving identity validation data cryptically in databases, establishing systems to perceive any uncontrolled change to be made, keeping adequate audit trail and providing the security of these audit trails. Furthermore, these data are encrypted while being transferred with the purpose of identity validation and measures are taken concerning the security of confidentiality during transfer of the data.

Incontestability and assigning responsibility

ARTICLE 10 —(1) The bank uses techniques including means of incontestability and segregation of duties for the critical transactions realized within the scope of information systems and of which scope to be determined by the bank.

Segregation of duties

ARTICLE 11 — (1) Segregation of duties and responsibilities principle is applied in improving, testing and processing system, database and practices relating to information systems, the duties and responsibilities assigned are reviewed periodically and if necessary updated in accordance with the segregation of duties principle. Processes and systems are designed so as to not to enable a critical transaction to be entered, authorized and completed by one personnel or support service institution.

(2) It is ensured that the personnel to carry out the processes that may have affect on bank data grants enough authority to execute only these duties for establishing an efficient segregation on duties environment having regard to the duties assigned to them.

(3) In cases where it is unlikely to decompose duties fully and appropriately, risk decreasing and controls are established to prevent error and abuses that may derive from this situation.

(4) Tests are conducted to determine if the controls established for providing requirements of segregation of duties principle in performing the functions relating to information systems are passable.

Authorization

ARTICLE 12 — (1) The bank establishes an appropriate authorization and access control for access to databases, practices and systems relating to information systems. Accordingly, authorization level and right of access are assigned appropriate to user, party and systems intervening to the activities realize in information systems. It is principle to assign the required lowest duty and grant the most limited right of access, having regard to duties and responsibilities of the related element in assigning authorization level and rights of access. Thus, it is enabled that only the user, party and systems having the necessary authority access

to systems, services and data. The duties to be assigned should be consistent with the principles which segregation of duties principle defines.

(2) Allocation of authorization and right of access mechanism is established in a way to disallow any user, party or system to increase their authorization level and rights of access above the levels defined beforehand.

(3) It is ensured that critical activities realized within the scope of information systems are performed upon the current and valid authorization databases. Authorities and rights of access assigned to all users, party and systems are subject to evaluation periodically in respect of appropriateness with the current situation. Security of authorization databases is provided and mechanisms are established to perceive any uncontrolled change to be made. Unauthorized access attempts to authorization databases are recorded and reviewed on a regular basis.

(4) Change, addition and erasing to occur in any database, practice and system including authorization databases relating to critical activities realized within the scope of information systems are ensured to be performed by authorized users of which identity validation is certified with appropriate techniques. An efficient change management is established under the structure of the bank for any transaction within this scope, sufficient audit trail is kept and the trails kept are reviewed regularly.

(5) In case the reliability of authorization databases relating to critical activities realized within the scope of information systems has lost, the related databases are not used unless changed back to current and reliable, allocation of authorization and right of access upon untrustworthy databases are not performed.

(6) Additional audit trails are kept for users and systems having privileged authorities and reviewed periodically.

(7) Users having privileged authorities made conscious adequately of the importance of preventing the usage of their authorities by other persons.

(8) For states of emergency, in authorizations realized temporarily due to failure to reach the authorized personnel, detailed audit trails are kept adequately to enable the transactions to be performed during this authorization process.

9) Controls and surveillance processes are established to prevent unauthorized physical and logical accesses relating to information systems infrastructure.

Consistency of transactions, records and locations (Amended OG-01/06/2010-27598) ARTICLE 13— (1) The bank takes the necessary measures to provide integrity of transactions, records and data to be realized through information systems and ensures accuracy, plentitude and trustworthiness of them. Measures relating to integrity are established so as to include the entire stages of transferring, processing and storing of the data. Same approach is adopted for the transactions realized by support service institutions.

(2) The plan is prepared for information systems services which support significant work functions in a way to consider the targets determined in work continuity plan.

(3) In preparation process of the plan, the impacts of interruptions determined within the scope of work impact analysis are analyzed by evaluating the level of significance of information systems assets and data kept. In accordance with the results of this analysis, a reasonable interruption period is determined for each service, alternative rescue procedures are developed that would enable the service to be opened for access again during this interruption and necessary measures are taken accordingly.

(4) Within the scope of the plan, performance pursue techniques are used, capacity planning is made, alternative channels are created against interruptions that could derive from network and communication infra-structure. In order to maintain sustainability of information systems, risk evaluation, risk decreasing and risk monitoring activities are carried out, scalability of information systems infra-structure capacity is analyzed in the light of general market dynamics and planned customer winning ratio, resistance of the system is tested by means of stress tests to be realized in accordance with transaction volume estimations.

5) Secondary center is established within the scope of the plan or agreements guaranteeing to procure the mentioned service from support service companies are made. Data and system back-ups are made ready for use in the secondary center pursuant to Article 11(4) of the Regulation on Internal Systems of Banks.

6) Implementing additional back-up to the provisions brought by this Communiqué is on the banks' own volition.

7) Plan is updated after revising the changes which will affect work process or information systems of Bank. Test are made in order to determine the efficiency and currency of the existing plan, support service companies are included to the tests, if any and test results are reported to the senior management.

Establishing audit trails

ARTICLE 14 —(1) Having regard to risks upon information systems, extent of the system and complexity of activities, an efficient audit trail record mechanism is established relating to the usage of information systems. Thus, it is ensured that audit trails realized within the scope of information systems and which cause change in records belonging to banking activities are kept in adequate detail and clarity. Necessary techniques are used so as to prevent deterioration of integrity of audit trails and if any, to determine any deterioration. Measures are taken so as to protect record system against any unauthorized systematic and user intervention. Audit trails are kept for transactions which cause change in records belonging to banking activities including information, as a minimum, relating to;

a) Unauthorized access attempts relating to the transactions within this scope,

b) Application realizing the transaction,

c) Identity of the person performing the transactions,

ç) Date of the transaction made.

(2) Audit trails of which extent is defined in paragraph one are kept by the bank for minimum 3 years. In addition to this, even if they cause no changes in records belonging to banking transactions, audit trails belonging to transactions on interrogating information that fall within the scope of confidentiality according to the Article 73 of the Law are kept by the bank for minimum 1 year, on the contrary to the provisions of the same article of the Law and in a way to enable the responsible ones are identified in case of disclosure of those responsible. It is ensured that audit trails are accessible for the period foreseen after the possible disasters that may occur by keeping in environments with sufficient security levels and are backed up.

(3) The bank informs its customers and personnel that the activities are recorded.

(4) The bank establishes processes relating to reviewing record system on a regular basis, evaluating records and reporting extraordinary situations to top-management.

(5) Keeping audit trails does not prejudice the responsibilities of the bank to keep the documents in accordance with other provisions of the legislation.

(6) In case of support service is procured within the scope of information systems, the bank ensures conformity of audit trails kept by the support service institution with its own standards and accessibility of audit trails hereof.

(7) Provisions included in this article relating to keeping information and documents are applied without prejudice to the related provisions of the other legislation on keeping information and documents.

Data confidentiality

ARTICLE 15 — (1) The bank takes measures to ensure the confidentiality of transactions realized within the scope information systems and data transferred, processed and protected within the scope of these transactions. The measures to be taken shall be appropriate to the confidentiality level of the transaction and data intended to be kept confidential and additional controls should be established. Studies conducted accordingly shall be in a character to meet the responsibilities of the legislation relating to confidentiality. Studies to be conducted to provide confidentiality, as a minimum, include;

a) Taking measures appropriate to the sensitivity of data by performing value and risk analysis, considering web and system structure, operations, extent and variety of the bank, during this analysis,

b) Accessing to data after a proper identity validation process by persons defined having regard to the segregation of duties principle and within the scope of the authorities foreseen in accordance with their responsibilities,

c) Taking algorithms proved to be trustworthy and sound as of the current situation for encryption techniques to be used in providing data confidentiality, selecting encryption keys to be used for related algorithms long so as not to be decrypted during the period which they are valid and can be used,

ç) Preventing the availability of invalid, stolen or decrypted encryption keys, determining the change frequency of keys according to materiality level of data and operation

d) Creating encryption keys securely, introducing to customer and personnel usage and protecting,

e) Recording accesses to banking data having confidentiality and protecting these records against unauthorized access and interventions,

f) Providing support service institutions within the scope of procurement of support services, to act in line with matters stated under this article and information security standards of the bank for situations which support service institutions have access to banking data.

Informing customers

ARTICLE 16 — (1) Customers to utilize from electronic banking/ alternative distribution canals (such as internet, telephone, television, WAP/GPRS, Kiosk, ATM) offered by the bank; are informed clearly about conditions on the services, risks and exceptional circumstances. In addition to this, security principles the bank adopted so as to decrease the risks relating to the said services and the necessary methods that should be used so as to protect from these risks are introduced to the attention of the customer.

(2) Mechanisms are established thorough which problems that customers may encounter due to information systems and services provided accordingly can be trailed and which enable customers to convey their compliments. Compliments and warnings conveyed are evaluated and studies are conducted to remove defects damaging the reputation of the bank.

Confidentiality of customer information

ARTICLE 17 — (1) The bank establishes the policy and procedures on providing confidentiality of customer information it acquired or protected by means of information systems while carrying out its activities, puts into writing, delivers to the related departments and takes the measures they require,

(2) Customer information within the scope of paragraph one can be shared with parties excluding components clearly authorized upon the laws, only if sharing limits are clearly defined and written approval of the customers are taken. The customers shall be offered

choices whether or not they share their information with the said parties and the customer needs to be informed on having such a choice.

Information systems continuity plan (Amended: OG-01/06/2010-27598)
ARTICLE 18- (Amended: OG-24/01/2009-27120*)* (1) Information systems continuity plan which is a part of work continuity management and plan set forth in Article 13 of the Regulation on Internal Systems is prepared so as to provide the continuity of information systems services that support the activities of bank.

(2) While preparing the permanence and rescue plan concerning the information systems; work impact analysis, risk evaluation, risk reducing and risk monitoring activities are realized.

(3) Tests are conducted regularly to ensure the efficiency and actuality of the present plan and the test results are reported to the senior management.

(4) The permanence and rescue plan concerning the information systems is periodically updated and reviewed after the changes that may affect them.

(5) Pursuant the provision within the fifth paragraph of the Article 13 of the Regulation on Internal Systems, necessary attention is shown to reduce the risks to minimum, in the selection of the place for the implementation of a data backup center. The primary target is that the real system and the backup center are not sensitive to the same risks.

(6) The Bank shall analyze the effects of possible interruptions by evaluating the criticality of information system assets and data collected. According to the analysis results of this effect, acceptable interruption durations for each service are determined, rescue procedures providing the opening to access to the service during this interruption are developed and necessary measures are taken.

(7) The Bank shall analyze the scalability the capacity of the infrastructure of information systems, in the light of general market dynamics as well as the planned customer winning ratios. The sustainability of the infrastructure is tested periodically by the stress tests realized in accordance with transaction volume estimations.

(8) While developing the permanence and rescue plan concerning the information systems, the related support service institutions are also considered if any, they are also included to the tests and the efficiency of the measures is controlled.

Emergency and Unexpected Events Plan

ARTICLE 19 — (1) The Bank shall take the necessary measures to manage the unforeseen events concerning the information systems and to reduce their effect to minimum, within the framework of the emergency and unexpected states plan regulated within the Article 13 of the Regulation on Internal Systems.

(2) For the scenarios predicted considering the presence and the effect of risk in the studies to be conducted within the scope of the first paragraph, a reaction process shall be implemented providing the conduct of the activities safely, effectively and regularly.

(3) The Bank shall implement the mechanisms which will provide the early information concerning the unexpected events related to the information systems.

(4) Within the scope of emergency and unexpected events plan, processes to find rapidly the source of the event concerning the information systems, to assess the damage, to show the potential dimension of the event as well as its effect, to provide its communication to the related management unit and to determine the affected customers are considered.

(5) **(Abolished by the OG-01/06/2010-27598)** The emergency and unexpected event plan includes also a communication strategy determining which channels of communication will be used between the bank and its customers and media organs. With this strategy, it is ensured that the bank’s customers and media organs are informed in time and correctly.

(6) For any kind of unexpected event to be realized concerning the information systems, the Bank shall implement a mechanism collecting the registries and information to be used during the administrative analysis, to ensure the subsequent analysis of the event. The registries collected shall also include the information which will provide the determination of the monetary loss.

SECTION TWO
Establishment and Follow-Ups of the Internal Controls Concerning Information Systems

Information Systems Controls

ARTICLE 20 — (1) The Bank shall implement the controls concerning the information systems expressed within the third paragraph of the Article 16 of the Regulation on Internal Systems in accordance with the Articles 21 and 22 of this Communiqué and shall follow them in accordance with the Article 23; to ensure the protection of its assets, the conduct of its activities actively and productively in accordance with the Banking Law and other related legislation, to policies and rules inside the banks as well as to banking conventions, the reliability and integrity of accounting and financial reporting systems and achievement of information in time.

Implementation controls

ARTICLE 21 — (1) The implementation controls include the internal controls required to be used in all working processes such as defining, producing, using the financial data used to conduct or support the banking activities within the information systems as well as ensuring their integrity and reliability and authorizing to achieve the data.

(2) Implementation controls are computer-assisted or manually realized specialized controls taking place within the working cycle expressing the control of the bank's working processes.

(3) The implementation controls include the following;

a) Data building /authorization controls:

1) Data preparing procedures: the entry form designs help to minimize the errors and deficiencies. The error handling procedures used in data building process ensure the detection, reporting and correction of errors and irregularities.

2) Source document authorization procedures: The authorized personnel prepare the source documents in accordance with their authorities. The building and approval of source documents is made in accordance with the distribution of duties principle.

3) Collection of source document data: Procedures ensuing the integrity and accuracy, as well as accountability and timeliness of the authorized source documents shall be found.

4) Handling the errors in the source documents: The error handling procedures used in data building process shall ensure the detection, reporting and correction of errors and irregularities.

5) Maintenance of source documents: To ensure that the data is achieved when necessary, procedures shall be determined to maintain the original source documents for a required time or to maintain them as to rebuild them.

b) Entry controls:

1) Entry authorization procedures: Procedures shall be determined ensuring that entries are made only from authorized sources.

2) Accuracy, integrity and authorization controls: Movement data produced by the personnel or by the system or entered from interfaces to be processed are made subject to several tests for accuracy, integrity and validity control. Furthermore, there shall be procedures to ensure that the entry data are changed and approved in the nearest place to the source point.

3) Handling the errors in data entries: There shall be procedures to ensure the correction and re-putting to process the data entered falsely.

c) Data-processing controls:

1) Integrity in data processing: The data processing procedures ensure that the distribution of duties principle is abided and that the works done are certified. These procedures also ensure the presence of adequate updating controls such as control sums from process to process and main files updating controls.

2) Approval and change in data processing: In data processing, there shall be procedures to ensure the approval, user certification and that changes are realized in the nearest place to source points.

3) Handling the errors in data processing: The procedures related to handling the errors in data processing assure that the false movements are detected before processing and prevent that they interrupt the valid ones.

d) Output controls:

1) Handling and maintenance of outputs: The determined procedures shall be followed in handling and maintenance of information system outputs and the confidentiality and security requirements shall be considered.

2) Distribution of outputs: The procedures relating to the distribution of information system outputs shall be defined, announced and being followed.

3) Output compatibility and agreement: The compatibility of the outputs with the control sums shall be controlled routinely. The audit trails facilitate the monitoring of operations concerning movements and to come to an agreement concerning the problematic data.

4) Reviewing the outputs and handling the errors: There shall be procedures to ensure the accuracy of output reports is reviewed by the people providing these outputs and adequate users. Moreover, there shall be procedures concerning the definition and handling the errors found in outputs.

5) Ensuring the security of the output reports: There shall be procedures to ensure the security of output reports distributed to users as well as reports waiting to be distributed.

e) Limit controls:

1) Authentication and integrity controls: the authenticity and integrity of the data produced outside the organization and received by phone, voice-mail, paper, fax or e-mail shall be controlled adequately before making any critical operation on the data.

2) Protection of sensitive information during its transmission and transport: During the transmission and transport, the sensitive information shall be protected from unauthorized access, modification and misdirection.

General controls

ARTICLE 22 — (**Amended: OG-24/O1/2009-27120**) (1) Information systems general controls are comprised of controls ensuring that the functions expected from information systems to be fulfilled accurately, targeting that a guarantee is established concerning the undesirable situations to be prevented, determined and corrected and for the functionality of implementation controls, and which are applied to all of the bank's information systems or to a part of it; as well as the policies and procedures ensuring the application of these controls. The general controls are the fundamental elements ensuring the establishment of the environment in which the bank's information systems realize their functions expected accurately, in time and confidentially.

(2) The Bank shall determine a universally-accepted standard, framework or methodology to establish the general controls and establishes them according to those. The standard, framework or methodology shall be determined considering the bank's activity scope and the weight and complexity of information systems used in activities. The standard, framework or methodology used by the Bank to establish its information systems general controls shall verify the control targets taken into consideration in COBIT, if there are deficiencies concerning this matter, the controls related to this shall be re-considered and established separately.

(3) The Bank shall establish environments adequate to the following matters concerning the each process subject to general control:

a) Owner of the process: An owner, responsibility of which is defined clearly, is assigned for each process subject to general control.

b) Repeatability: The processes subject to general control are defined as to be repeatable.

c) Targets and objectives: Clearly defined targets and objectives shall be formed for each process subject to general control, to ensure that they operate efficiently.

ç) Roles and responsibilities: Roles, activities and responsibilities shall be defined clearly for each process subject to general control, to ensure that they operate efficiently.

d) Process performance: The performance of each general control process is measured according to the determined targets.

e) Policies, plans and procedures: Policies, plans and procedures concerning each general control process are put into writing, reviewed regularly, updated, approved and announced to all related units.

Follow-up of Controls

ARTICLE 23 —(1) As a part of the internal control activities implied within the Regulation on Internal Systems, together with the efficiency, adequacy and compatibility of the information systems controls, its performance in reducing the effect of risk or risks targeted with the control is continuously followed-up and evaluated. Important control deficiencies detected as a result of the evaluation are reported to the senior management or to relevant committees and necessary measures are taken.

SECTION THREE
Special Transactions

PART ONE
Internet Banking

Provisions to be used in internet banking

ARTICLE 24 — (1) The provisions taken place in this part are valid only for internet banking services enabling to see or change the financial or personal information belonging to the customer or to realize transactions creating financial responsibility. All sorts of infrastructure concerning the internet banking are considered as a part of the bank's information systems. Accordingly, the provisions taken place within the other parts of the Communiqué are also valid for the studies made within the scope of internet banking. The

provisions included within the articles under this section are considered as addition to the provisions included within the articles having the same titles under the Part One of the Section Two of this Communiqué.

Surveillance of the management

ARTICLE 25 — (1) It is taken into consideration that the banking services presented within the scope of internet banking activities will be exposed to some additional risks emanating from the nature of the internet, such as not providing the security, not determining the identification accurately, possibility to deny and not assigning any responsibilities; additional controls are established in accordance with the provisions within the articles 26 to 31 of this Communiqué for the processes related to these services.

Establishment and management of Security control Process

ARTICLE 26 — (1) To test the adequacy of security controls, infiltration tests are made to systems within the scope of internet banking activities by independent teams for at least once a year.

(2) The Bank shall establish necessary following-up mechanisms to detect the extraordinary and suspicious transactions realized within the scope of internet banking activities.

Identity Validation

ARTICLE 27 — (1) The Bank establishes a trustworthy ID verification mechanism compatible to risk levels presented by the internet banking services provided by the Bank. An infrastructure not permitting that the customers procure from services without passing through these ID verification mechanisms shall be established by the Bank.

(2) For determining the risk levels for the services, the following shall be considered as a minimum;

a) Customer type,

b) Operational possibilities presented to the customer,

c) Sensitivity of the information shared between the Bank and the customer,

ç) Communication infrastructure used and

d) Transaction volume.

(3) ID verification operation for internet banking is realized for all intervening parties, such as the bank, customer and if any, the support services institution, intervening to the transaction.

(4) The ID verification mechanism applied to customers is composed of at least two different components independent form each other. These two components are chosen as to belonging to two of the element classes which are “known” by the customer, “owned” by the customer or “which is a biometric characteristic” of the customer. For the element “known” by the customer, components such as password/changeable password may be used, for the element “owned” by the customer, a changeable password producing device, changeable password procured by SMS service may be used. The components shall be entirely special to the customer and the ID verification shall not be realized and the services shall not be accessed without presenting those components.

(5) In case of electronic signature usage in ID verification, only if the secure electronic signature provisioned within the Article 4 of the Act on Electronic Signature Nr. 5070 dated January 15, 2004 is used; it is considered that the provisions within the fourth paragraph of this Article are fulfilled. If in ID verification through electronic signature, foreign electronic certificates are used, the provisions within the Article 14 titled “Foreign Electronic Certificates” of the Act mentioned in this paragraph and within other related regulations are valid.

(6) A policy shall be determined for the management of the passwords and changeable passwords to be used in ID verification of the customers; this policy shall include at least the following;

a) Passwords and changeable passwords shall be in a complexity and longitude difficult to guess and break; the customers shall be obliged systematically to provide this complexity in determining their passwords and changeable passwords,

b) Changeable passwords shall be used for a determined period and shall be out of use by the end of this period and the customer shall be obliged o choose another changeable password; the new changeable password shall not be accepted by the system unless it is different form a number of passwords used recently,

c) The operations to initialize the password and the changeable password shall include adequate security controls,

d) Customers shall be informed about the importance of determining adequate passwords and changeable passwords and ensuring their confidentiality.

(7) The coding techniques to be used in ID verification shall be based on algorithms accepted actually in the literature and which have not lost their confidentiality. The encoding keys to be used shall be long enough, during the time period in which the key for related algorithms will be valid and be used, they shall not be broken. The use of invalid, stolen or broken encoding keys shall be prevented.

(8) The encoding keys used in ID verification shall be presented to the use of customers as to include the methods which will ensure that; the possibility to obtain these keys is minimum, the confidentiality is provided, and preventing that their modification and corruption. When the encoding keys are used for ID verification, they shall be accessible by a password, PITN (Personal Identification Number) or biometric component information.

(9) If the customer is asked for transaction verification code for realizing the transactions within the scope of internet banking, the verification codes shall be composed of enough alphabetical and/or numerical characters as to be difficult to guess, they shall be created randomly and they shall be sent to the customer via a communication environment other than the internet. The transaction verification codes shall be produced flexible and unique to prevent guessing.

(10) The information on the devices presenting changeable password shall be erasable in a determinant period and/or shall be cleared from the device by a cleaning possibility; the passwords produced by these devices shall be impossible to guess by password guessing methods known, flexible and unique.

(11) The security of the components to be used in ID verification mechanism of customers such as password, variable password, changeable password device, secret coding key smartcard and transaction verification code shall be provided during the whole process starting from their production until their access to the customer and the Bank shall be sure that their confidentiality is not tainted when they are brought into the use of customer.

(12) The Bank shall verify that the source of all kinds of software presented by the Bank to the customers to be used in transactions within the scope of internet banking is the Bank and the controls verifying that these software do not include any kinds of codes which may put in danger the user security are conducted by the Bank.

(13) The ID verification mechanism established by the Bank;

a) Shall give information concerning unsuccessful ID verification attempts to the related customer on the moment he/she enters to the system, and block the access to internet banking after a determined number of unsuccessful attempts,

b) Shall not give any unnecessary information after the unsuccessful ID verification attempts to the person who realized these attempts, about falsely entered user information or password/changeable password, for example declaring that there is not such a user within the system or that the password/changeable password is entered falsely.

(14) The Bank shall take necessary systematical measures and measures concerning the software face to the known attacks of obtaining the ID verification information regarding the customers and personnel, in the systems to be established as well as the applications to be developed.

(15) To determine the possible threats and to take necessary measures, the successful and unsuccessful access attempts to the accounts of internet banking are regularly followed-up by the Bank, when a proportional anomaly is detected, it shall be investigated.

Incontestability and assigning responsibility

ARTICLE 28 - (1) The Bank shall use the techniques and establish the controls to enable the restoration of incontestability and assignment of responsibility for the transactions realized within the scope of internet banking activities. The techniques to be used and the controls to be established shall ensure that both the bank and the customer does not deny the transactions realized by the party who started it and the party who finished it in all kinds of transactions emanating financial results. The audit trails formed by the technique used or the controls established shall constitute evidence and assign responsibility.

(2) The techniques may be based on ID verification mechanism or be integrated to it; or may be devoted entirely to incontestability and responsibility assignment.

(3) The internet banking service presented by the Bank shall be organized as to include the necessary controls reducing the possibility of customers to make wrong transactions and shall ensure that they understand the risks concerning their transactions completely.

Establishing audit trails

ARTICLE 29 — (1) The Bank shall establish a sufficient and efficient mechanism to keep audit trails for all the internet banking activities. The Bank shall at least keep audit trails concerning;

a) Account opening, closing and modification of account,

b) Transactions bearing financial results,

c) Limit exceeding approvals given for the customer,

d) All kinds of modifications made in rights, privileges, and constrain regulating the access to the Internet banking system.

The audit trails shall include detailed information to show the source and the course of the transaction from beginning until the end.

(2) The Bank shall ensure that the record keeping processes and infrastructure concerning the internet banking activities is structured as to produce evidences and prevent the deterioration of these evidences, to distinguish the misleading evidences and to present the information in assigning responsibility to the parties.

(3) The provisions concerning information and document keeping within this article are applied on condition that the provisions concerning information and document keeping within other related legislation are kept reserved.

Informing the customers

ARTICLE 30 — (1) The Bank shall inform its customers about the present policies and procedures concerning the internet banking service and shall issue necessary warnings.

(2) The Bank cannot open the internet banking service to usage for a customer without having the customer's demand. If the customer has closed or made closed his/her access to the internet banking service, the internet banking service cannot be open to usage without the demand of the customer.

(3) In the website in which the internet banking service is procured, the Bank shall use the techniques showing that the website belongs to the Bank.

(4) The Bank shall introduce information about its identity and legal status on the website in which it presents internet banking services. Within this scope, the Bank shall give information concerning as a minimum:

a) Commercial title of the Bank, the address of its head office,
b) Communication information concerning the Banking Regulation and Supervision Agency which is responsible for the supervision of the Bank,

c) Information concerning the conditions and scope of insurance of the deposit.

(5) The Bank is responsible for;

a) Presenting clear and understandable information about the risks carried as well as the favors gained by the internet banking services and the responsibilities and rights of customers benefiting from internet banking services,

b) Bringing the policies and procedures concerning the confidentiality of the customers' personal information to the customers' attention, by paying also regard to bank security,

c) Informing the customers, about whom services are given under the internet banking as well as the conditions to access these services and security requirements,

d) Publishing security guides aiming to create awareness of customers and bringing the policies and procedures about this subject to the customers' attention by also paying regard to bank security,

e) Informing the customers about the modifications made in the internet banking system or in the website in which the internet banking service is procured, and which may affect the accessibility.

(6) The Bank shall also inform its customers about following matters;

a) How to use the services procured within the scope of internet banking service,

b) What shall customers do to realize their transactions safely upon the internet banking, what to pay attention in choosing passwords or variable passwords and the responsibilities of customers in furnishing the safety of these passwords,

c) What to do if there is a problem,

d) Conditions concerning each service procured and taken; clear definition of the responsibilities and duties of the parties, without giving place to any hesitations.

(7) Any kinds of explanations defined within the scope of this article and aiming to inform the customers is kept open to the customer's access on the website in which the Bank is offering the internet banking service. All explanations shall be as clear and understandable as possible. The explanations shall be placed in a remarkable place on the website in which the internet banking is procured and there shall be orientations and systematical constraints to guarantee that the customers read them at least for once.

(8) The Bank shall avoid the expressions giving the impression or information that the internet banking services are absolutely safe or there are no risks in internet banking services in the marketing activities, advertisements and publications. The customers are warned about the risks and threats of the internet banking and maximum effort shall be made to raise the awareness of the customers.

(9) For the internet banking transactions realized by mobile communication devices, the informing necessities mentioned under this article are valid. If these devices are remain incapable to procure related information, necessary orientation to provide that the customer obtains this information through another channel.

Service continuity and rescue plan

ARTICLE 31 — (1) The Bank shall procure service continuity in a level declared for the internet banking or committed to the customers. The Bank shall take necessary measures to minimize the legal responsibilities which may be emanated from service disconnections.

(2) The Bank shall not make disconnections without announcing previously the customers, unless there are compelling reasons, The Bank shall announce the disconnections occurring in the internet banking services in advance and shall inform the customers about the reasons of this disconnection.

(3) While developing service continuity and rescue plans, the attacks of putting out of operation shall be taken into consideration, necessary measures are taken face to them.

PART TWO
ATM

ATM security

ARTICLE 32 — (1) The Bank shall establish measures to minimize the risks concerning ATM devices such as burglary, fraud, physical assault and create awareness by the customers about the safe usage of ATM devices.

(2) All kinds of passwords/changeable passwords came predefined on the ATM devices shall be changed as to be unpredictable to prevent that the ATM device is managed by malicious persons knowing the passwords/changeable passwords.

(3) Necessary measures preventing malicious persons to load programs with bad content to ATM devices as well as unauthorized access, all entry points providing the unauthorized persons to attach another electronic device to the ATM shall be closed. Necessary updates and patches shall be loaded automatically or regularly to the ATMs to correct the security gaps. Additional security measures shall be taken to prevent the connection of other devices in an unauthorized way to the network between the ATM and the Bank.

(4) The communication network used for the transactions realized on the ATM devices shall be qualified as to provide data safety, confidentiality and integrity. The PIN information entered by customers as well as the information concerning the transactions realized shall be transmitted in a coded way through the ATM network inside and outside the machine.

(5) The ID verification mechanism applied to customers shall be formed by at least two components independent from each other. These two components; are chosen as to belong to

two of the elements which are “known” by the customer, “owned” by the customer or “is a biometric characteristic” of the customer. Components such as PIN information may be used for the element “known” by the customer, or as ATM card may be used for the element “owned” by the customer. The components shall be entirely personal and ID verification and the access to the services shall not be realized unless these are presented.

(6) To provide the service continuity of the ATM devices and to detect early the risks they may be exposed to such as fraud and physical assault, a remote administration and monitoring system shall be established by the Bank for the ATM device.

(7) The ATM operators and technicians are trained about all of the actual fraud methods concerning the ATM devices and these personnel shall regularly control the ATM devices. The ATM devices shall be regularly and attentively investigated face to the possibility of installation of foreign equipments or other electronic devices (card copying devices, fake keyboard, camera, etc.) on them.

(8) The negotiations concerning the ATMs shall be realized by at least two persons in sufficient frequency and according to the distribution of duties principle.

(9) To ensure that its customers are benefiting safely from the ATM services, the Bank shall inform them about ATM security and protecting themselves from actual fraud methods and creates awareness by the customers about this subject.

(10) The Bank shall install a security camera to the place where the ATM is placed, but this camera is positioned as to the keyboard movements of the customer are not seen. The security camera records are maintained at least for two months and the camera equipments are controlled regularly to see if they operate. If there is a security camera infrastructure covering the conditions mentioned in this paragraph, and embracing the ATM by its recording field, there is no need for an extra security camera for the ATM. Furthermore, the condition to install a security camera for the ATMs taken place within the activity field of public security and intelligence institutions is fulfilled only if the necessary permissions are granted from the related public security and intelligence institutions.

SECTION FOUR
Miscellaneous and Final Provisions

PART ONE
Miscellaneous Provisions

Wireless communication technologies

ARTICLE 33 — (1) The Bank shall take necessary measures to manage the risks relating to the wireless communication technologies used in both execution of general banking activities and establishment of alternative distribution channels, in its information systems infrastructures. The management of risks related to the use of wireless communication technologies in banking activities is considered as a component of the information systems management. The weaknesses of wireless technologies are also considered and necessary controls are established.

Situations not provisioned by the Communiqué

ARTICLE 34 — (1) In case of situations not provisioned by this Communiqué; the principles and procedures taken place within the Regulation on Internal Systems as well as the principles and procedures taken place within the COBIT documents presenting the internationally accepted information technologies control targets are applied.

PART TWO
Final Provisions

Transition Process

PROVISIONARY ARTICLE 1 — (1) The Bank shall align its present activities and systems with the provisions of this Communiqué, within maximum two years after the date of promulgation.

Entry into Force

ARTICLE 35— (1) This Communiqué enters into force as of January 01, 2008.

Enforcement

ARTICLE 36 —(1) The provisions of this Communiqué are enforced by the Chairman of Banking Regulation and Supervision Agency.