COMMUNIQUE ON INFORMATION SYSTEMS USED IN PAYMENT AND SECURITIES SETTLEMENT SYSTEMS (No. 2015/7)

SECTION ONE

Objective, Scope, Legal Basis and Definitions

Objective

ARTICLE 1 – (1) The objective of this Communique is to regulate the procedures and principles regarding information systems which are used for carrying out activities related to payment and securities settlement systems.

Scope

ARTICLE 2- (1) This Communique, with respect to information systems which are used for carrying out activities relating to payment and securities settlement systems, shall contain procedures and principles regarding general provisions on information systems management, data security management, security vulnerabilities and violations, audit trails, identity authentication, access control and non-repudiation, information systems risk management, information systems operation, information systems continuity plan, outsourcing for information systems and other related matters.

Legal basis

ARTICLE 3- (1) This Communique has been prepared on the basis of the third paragraph of Article 4 of the Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions No. 6493 dated 20 June 2013, the ninth paragraph of Article 24 and the first paragraph of Article 30 of the Regulation on Operations of Payment and Securities Settlement Systems published in the Official Gazette No. 29044, dated 28 June 2014.

Definitions

ARTICLE 4 – (1) In this Communique, the following terms shall have the meanings indicated below:

a) Bank: The Central Bank of the Republic of Turkey Joint Stock Company,

b) Information systems: Entire structure composed of hardware, software, data and processes that ensures the fulfillment of system operators' information and data related responsibilities set out by legislation in order to carry out activities regarding payment and securities settlement systems,

c) Information systems continuity plan: A plan that contains the scenarios regarding all kinds of extreme circumstances including cyber-attacks that may negatively affect the uninterrupted operation of information systems and the provisions for recovering from disruptions that could occur in information systems in reasonable time and without any data loss if these scenarios are realized,

ç) Information systems management: Activities regarding the establishment of appropriate information systems, the effective and efficient usage of information systems resources, the management of information security, the management of risks associated with information systems and the maintenance of the continuity of information systems in order to ensure

uninterrupted, safe, effective and efficient functioning of payment and securities settlement systems,

d) Change management: A service management discipline for information systems that aims to ensure that all changes related to information systems are made on time and in an effective and safe manner, and to minimize the number of the incidents arising from these changes and the impact of these incidents on the services by using pre-defined procedures,

e) Audit trail: Records that enable to follow a financial or operational transaction step by step from its beginning to its end,

f) Regulation on operations: Regulation on Operations of Payment and Securities Settlement Systems that is published in the Official Gazette dated 28 June 2014 and No. 29044,

g) Service level: A level regarding the content and quality of services, which is predetermined in written form and shared with relevant parties by the system operator by taking into consideration the cost of services and the requirements and expectations of beneficiaries of these services,

ğ) Capacity management: Activities that involve monitoring current capacity and performance of information systems, conducting tests including stress tests for information systems, planning information systems by reviewing them in accordance with the business needs, technical requirements and business continuity objectives,

h) Participant: A legal person with the right to give a direct transfer order by participating in the system and obliged to comply with the system rules,

ı) Securities settlement system: The structure that has common rules and provides the infrastructure required for the clearing and settlement transactions carried out in order to realize securities transfers arising from transfer orders among three or more participants,

i) Incident: Any kind of event that causes an unplanned outage in the operation of

information systems or a decrease in service quality including security violations,

j) Payment system: The structure that has common rules and provides the infrastructure required for the clearing and settlement transactions carried out in order to realize fund transfers arising from transfer orders among three or more participants,

k) Project management: A process that ensures the planning, organization and execution of information systems projects in a way that enables the completion of these projects in accordance with a projected time plan, budget and quality level by using the predetermined methodologies,

l) Penetration test: The activities that include attacks on information systems in order to detect and fix security vulnerabilities, if any, before being exploited,

m) System: Payment system and securities settlement system,

n) System operator: Legal person responsible for the daily operations of the system and holds the required license for operating a system,

o) Problem: Root cause of one or more incidents,

ö) Stress test: A test that measures the sufficiency of the capacity of information systems under the circumstances in which the information systems are exposed to loads heavier than the peak load,

p) Person responsible for management: Persons, defined in Article 10 of Regulation on Operations and who are responsible for the management of the system operator,

r) Vulnerability scan (analysis): Analysis that is usually performed via automatic tools in order to detect, identify and classify security vulnerabilities, if any, in the components of information systems in advance.

SECTION TWO

Principles on Information Systems Management

General provisions regarding information systems management

ARTICLE 5- (1) The system operator shall primarily consider the objective of uninterrupted, safe, effective and efficient functioning of the system for which it is responsible, while performing its activities regarding information systems.

(2) The system operator shall establish information systems in compliance with the system's field of activity and update them by taking into account technological developments.

(3) The system operator shall determine policies regarding information systems management in accordance with its main strategies and targets related to the system in written form, review these policies on a regular basis, and update them if necessary.

(4) The system operator shall perform the management of the system with a holistic approach and within the scope of the corporate governance practices in a way that covers information systems management, and locate the elements of information systems management to the appropriate places in the organizational structure.

(5) The system operator shall clearly determine the duties, powers and responsibilities in relation to information systems management and provide all kinds of resources required for information systems management.

(6) The board of directors of the system operator is responsible for conducting information systems management which is compatible with the provisions of this Communique.

Information security management

ARTICLE 6 – (1) The system operator shall establish an information security management framework that includes rules, principles and policies to ensure confidentiality, integrity and availability of all kinds of information assets regarding the system.

(2) The system operator shall establish an information security management system that is compatible with the information security management framework constituted within the scope of the first paragraph.

(3) The system operator shall clearly define duties, powers and responsibilities for establishing, managing, periodically reviewing and if necessary updating the information security management system.

(4) Within the scope of the information security management system, duties, powers and responsibilities of personnel at every level with regard to information security shall be clearly defined.

(5) The system operator shall classify all information assets in the system according to their confidentiality level by also taking criticality and legal obligations into consideration; shall clearly define access rights and procedures regarding storage, transmission and disposal of

information assets at every level, and shall inform all personnel about classification of the information assets and obligations with respect to classification.

(6) All issues regarding personnel including inauguration, change of duty and position and termination of employment shall be assessed with respect to their impacts on information security and necessary measures shall be taken within the context of the information security management system.

(7) The system operator shall ensure the security of all kinds of system related hardware and infrastructures and their physical environment which are located in its own property within the scope of the information security management system. The system operator shall exercise due diligence to ensure the security of all kinds of system related hardware and infrastructures and their physical environment which are not located in its own property.

(8) The system operator shall ensure that all kinds of communication processes and operational transactions regarding main activities, which occur between internal and external networks with regard to the system, are designed in a way that these processes and transactions take place by using security controls and tools.

(9) The system operator is obliged to pay necessary attention to information security while establishing a new system, making a structural change in existing systems or conducting the development, maintenance and restoration activities on current information systems.

(10) The persons responsible for the management of the system operator and to whom duties, powers and responsibilities are given regarding the information security management system, shall continuously monitor the information security management system's compliance with legislations and standards about information security and the information security management framework which is constituted within the scope of the first paragraph, shall take necessary measures to ensure its compliance and report the compliance level to the board of directors of the system operator.

(11) The system operator shall carry out the necessary activities to enhance personnel's awareness of information security issues.

Security vulnerabilities and violations

ARTICLE 7 – (1) The system operator, in accordance with the information security management framework, shall ensure that potential security violations with regard to information systems are investigated, appropriate measures to prevent security violations are determined, necessary measures to timely detect and respond to the violations are taken when security violation occurs, and realized security violations, and identified security vulnerabilities are analyzed and recorded.

(2) The system operator shall perform vulnerability scans on all owned system related servers and communication networks, before their first startup and on a regular basis at least six times a year thereafter. It shall be ensured that critical findings detected in vulnerability scans are removed as soon as possible and appropriate protective measures are taken until these findings are removed. A time plan shall be prepared in order to remove noncritical findings in a reasonable time period.

(3) The system operator shall ensure that a penetration test is conducted at least once a year, in accordance with the scenarios including potential internal and external threats and shall report the results of the penetration test to the Bank.

(4) The system operator shall take appropriate measures regarding the assessment of potential and occurred security violations and removal of security vulnerabilities detected during vulnerability scans and penetration tests, and shall control the effectiveness of these measures.

(5) The system operator shall present a report to the Bank at least once a year that includes occurred security violations and detected critical security vulnerabilities, measures taken for the removal of these vulnerabilities and results of these measures.

(6) The system operator shall keep the evidences related to the occurred security violations safely for at least ten years.

Audit trail recording system

ARTICLE 8 – (1) The system operator shall establish an audit trail recording system that enables the tracking of all kinds of authorized or unauthorized access to information systems and transactions executed in information systems with regard to system activities.

(2) Depending on the nature of the transaction or access, records that will be kept on the audit trail recording system shall contain at least transaction type, unique transaction identifier, value of transaction, transaction date, transaction time, user identity information and information about application on which the transaction or access took place.

(3) Audit trails shall be kept for at least ten years in a form that is secure, ready for audit and enabling detailed examination and scanning.

(4) In case the system operator outsources information systems, the system operator shall be responsible for the compliance of audit trail recording system of the outsourcing service provider with provisions of this Article.

Identity authentication, access control and non-repudiation

ARTICLE 9 – (1) The system operator shall establish a sufficient and effective identity authentication system which will be used for transactions executed in information systems.

(2) The system operator shall clearly determine to which subcomponents of information systems the identity authentication system will be applied and which identity authentication methods will be used for which subcomponent in the identity authentication system.

(3) The system operator shall clearly identify the authorizations and restrictions of personnel regarding their access to networks, subsystems, applications, data and physical environments used within the system in a way that allows their access to the information necessary for their tasks within the scope of their duties, powers and responsibilities, and shall take necessary measures to prevent unauthorized access.

(4) The system operator shall ensure the establishment of necessary infrastructure for the safety, and encrypted transfer and storage of data used for identity authentication.

(5) The system operator shall take measures to ensure the safety of session during usage of information systems.

(6) The system operator shall establish technological and legal infrastructure which will ensure non-repudiation for operations executed in information systems regarding system activities.

Information systems risk management

ARTICLE 10- (1) The system operator shall take into account the risks regarding information systems while designing risk management framework in order to identify,

measure, monitor and effectively manage all risks which may adversely affect the smooth operation of the system.

(2) While assessing the risks regarding information systems with respect to the first paragraph of this Article; the main activities and other activities of the system operator, the activities of participants and other institutions that directly or indirectly connect to the system, the activities of outsourcing service providers and, if any, the interdependencies with third parties and the interconnections with other systems shall be taken into account.

(3) The system operator shall perform a comprehensive risk assessment regarding information systems at least once a year and submit a report that includes the results of this assessment to the Bank.

Operation of information systems

ARTICLE 11 – (1) The system operator shall clearly determine the objectives related to reliability, resiliency and continuity of information systems' operations within the scope of defined service-levels and in line with these objectives shall take necessary measures for ensuring the effective and efficient operation of information systems.

(2) The system operator shall assess the compliance level with the objectives determined within the scope of the first paragraph at regular intervals at least once a year and report the results to the Bank.

(3) The system operator shall establish its information systems in a way that will ensure that it has sufficient capacity for the defined service-levels and shall primarily consider that the capacity is scalable and shall employ capacity management for its information systems.

(4) The system operator shall ensure the constitution, safekeeping, updating and reporting of inventory and configuration of the information assets.

(5) The system operator shall implement incident management with respect to predetermined procedures, in a way which ensures that the incidents are timely detected, recorded, reported, analyzed, resolved and all relevant shareholders are informed about the incident on time.

(6) The system operator shall implement problem management after every major incident in a way that includes detailed incident investigation, performing root cause analysis, identifying the impacts, and tracking and reporting of the problem related to the event.

(7) The system operator shall make all necessary changes related to information systems in accordance with the predetermined change management procedures.

(8) The system operator shall carry out all kinds of information systems projects; either developed in-house or outsourced, in accordance with predetermined project management procedures.

Information systems continuity plan

ARTICLE 12 – (1) The system operator shall prepare an information systems continuity plan as part of the business continuity plan that is constituted in accordance with the fifth paragraph of Article 25 of the Regulation on Operations.

(2) The information systems continuity plan contains;

a) Information systems continuity objectives that will be determined in line with the business continuity plan and the backup and recovery procedures which will be established to ensure achievement of these objectives and also the resources that will be used.

b) Processes that ensure the detection of the source of, the damage created by, the potential size and impact of the incident which caused the implementation of the plan, and the parties affected by this incident and the notification of the detected findings to related management units.

c) Criteria and procedures that are related to decision making process for the activation of the plan and duties, powers and responsibilities of the persons or the groups who will take role when the plan comes into effect.

ç) Communication method with relevant stakeholders,

d) Recording method for the decisions taken and the actions performed within the scope of the plan.

(3) The system operator shall test the effectiveness of the information systems continuity plan at least once a year. The system operator shall plan these tests by also including the participants, other systems which have linkages to information systems and third-party service providers.

Outsourcing regarding the information systems

ARTICLE 13- (1) The system operator may outsource activities regarding the information systems. The outsourcing does not abolish the responsibilities of the system operator regarding the information systems management.

(2) The system operator shall assess the risks which may arise from outsourcing and take necessary measures.

(3) The outsourcing contract shall at minimum include the following;

a) Issues regarding the scope of the service and the determined service levels,

b) The conditions regarding the termination of the outsourced service and, in case this service ends, the provisions regarding the destruction of the information, documents and records obtained by the outsourcing service provider while providing this service,

c) The rights and obligations of the system operator and the outsourcing service provider,

ç) The provisions which will ensure the compatibility of the sources and processes used by the outsourcing service provider with respect to the relevant service to the security policies of the system operator,

d) Issues with regard to the ownership and the intellectual property rights of the elements subject to the contract,

e) The provisions regarding the ownership of the information, documents and records related to the transactions realized via outsourcing belongs to the system operator and provisions regarding the confidentiality of the system operator’s information, documents and records,

f) The provisions mentioning that the term of the contract are binding also for the contract, if any, between the outsourcing services provider and its subcontractors,

g) The provisions that ensure the outsourcing service provider will make the necessary changes that shall be done in information systems by the system operator pursuant to the regulations and Bank orders to which it is subject to because of its feature as a system operator,

ğ) The provisions clarifying that the operations conducted via the outsourcing service provider are also in the scope of the Bank’s oversight activities carried out for the system operator and that the outsourcing service provider is obliged to give all requested information,

documents and records in a timely and accurate manner and to ensure any kind of facility necessary to access them,

h) The provisions to be followed in case the contract provisions are violated for any reason.

(4) In case that the system operator outsources the processing and storage of data, this service shall be provided to the system operator only through dedicated hardware.

(5) When outsourcing, the system operator shall take necessary measures to ensure the security of its own and its participants' information and provide the outsourcing service provider authority with access only to the information which is required to be accessed with respect to the nature of the work.

SECTION THREE

Miscellaneous and Final Provisions

Implementation principals

ARTICLE 14 – (1) The Bank is authorized to construe the provisions of this Communique, to make a decision about the issues which are not mentioned or not explicit in this Communique by taking into account the general provisions, to publish circulars and mandates to regulate and to direct the implementation.

Transitional provision

PROVISIONAL ARTICLE 2 – (1) The system operators are obliged to harmonize their systems with this Communique within one year as of the date of publication of this Communique.

Enforcement

ARTICLE 15- (1) This Communique shall enter into force as of the publication date.

Execution

ARTICLE 16 - (1) The provisions of this Communique shall be enforced by the Governor of the Central Bank of the Republic of Turkey.