Decision

on adequate information system management

(Official Gazette 37/2010)

Pursuant to Article 161, paragraph (1), item (3) of the Credit Institutions Act (Official Gazette 117/2008, 74/2009 and 153/2009) and Article 43, paragraph (2), item (9) of the Act on the Croatian National Bank (Official Gazette 75/2008), the Governor of the Croatian National Bank hereby issues the

Decision on adequate information system management

1 GENERAL PROVISIONS

Article 1

(1) This Decision governs the obligations of credit institutions relating to information system management.

(2) This Decision shall apply to:

1) credit institutions which have their registered offices in the Republic of Croatia and which are authorised by the Croatian National Bank and,

2) branches of third country credit institutions authorised by the Croatian National Bank to provide services.

(3) Notwithstanding paragraph 2 of this Article, this Decision shall not apply to electronic money institutions.

2 DEFINITION OF TERMS

Article 2

1) *Software components* (software assets) include application software, system software, databases, software development tools, utility programs and other software.

2) *Hardware components* (hardware assets) include computers and computer equipment (stationary and mobile personal computers, servers, monitors, keyboards, printers, etc.), communication equipment (routers, switches, firewalls, etc.), data storage media (magnetic discs, magnetic tapes, optical discs, etc.), and other technical equipment supporting the information system operation (uninterrupted power supply devices, air-conditioning facilities, etc.).

3) *Information assets* include data in databases, data files, source code, system and application documentation, user manuals, plans, internal bylaws, etc.

4) *Information technology* ensures automated collection, processing, generating, storage, transmission, presentation and distribution of information, and the disposal thereof. The information technology comprises software and hardware components.

5) *Information system* is a total of technological infrastructure, organisation, human resources and procedures for the collection, processing, generating, storage, transmission, representation and distribution of information and the disposal thereof. The information system can also be defined as an interaction between information technology, data and data processing procedures and the people collecting and using these data.

6) *Information system users* are any persons using the information system (a credit institution's employees, a service provider's employees, electronic banking users, legal persons' employees using a credit institution's information system, etc.).

7) *Information system risk* is a risk arising from the use of information technology or information system.

8) *Information system resources* include information assets, software components and hardware components.

9) *Properties of information and processes* include confidentiality, integrity, availability, authenticity, non-repudiation, verifiability and reliability.

10) *Confidentiality* is a property of information (data) implying that it is not made available or disclosed to unauthorised parties.

11) *Integrity* is a property of information (data) and processes implying that it has not been subject to unauthorised or unforeseen alterations.

12) *Availability* is a property of information and processes implying that these information and processes are accessible and usable, i.e. available to an authorised party at its request.

13) *Authenticity* is a property implying that a party's identity is as claimed.

14) *Non-repudiation* is a property implying the inability to deny having performed an action or received some information (data).

15) *Verifiability* is a property that allows a party's activities to be tracked directly to the party itself.

16) *Reliability* is a property implying consistent and expected behaviour and results.

17) *Controls* are divided into administrative, logical and physical controls.

18) *Administrative controls* include the adoption of internal bylaws relating to the information system and setting up of an appropriate organizational structure, and ensure the implementation of internal bylaws relating to the information system, with a view to ensuring its functionality and safety.

19) *Logical controls* are the controls implemented in the software components of an information system.

20) *Physical controls* are the controls protecting the information system resources from unauthorised physical access, theft, physical damage or destruction.

21*) User access rights management* includes registration, authorisation, identification, authentication and the supervision of user access rights.

22) *Enrolment* is the process of defining new information system users.

23) *Authorisation* is the process of assigning access rights to information system users.

24) *Identification and authentication* are the processes by which an information system user is identified and his/her identity verified at registration and during the operations performed on the information system.

25) *The supervision of user access rights* is a process that includes the monitoring, altering and revision of information system users' access rights.

26) *User identity* can be verified in one, or a combination, of the following ways:

(a) by means of something which is only known to the user (e.g. password, PIN or cryptographic key);

(b) by means of something which is owned by the user only (e.g. magnetic card, chip card or token);

(c) by means of something that user knows, is or has (using the biometric methods, such as fingerprint check, iris scan, voice or handwriting recognition, etc.).

27) *Administrative access to information system* is the access to the information system resources provided to information system users with wide authority and administrative access enabling them to avoid built-in logic controls including, among others, database administrators, network administrators, system administrators and application software administrators.

28) *Remote access to a credit institution's information system resources* is the access to such resources from a remote location by using a telecommunication infrastructure which is not fully controlled or supervised by the credit institution.

29) *Audit trails (logs)* are chronological records of operations performed on the information system resources (operation system log, firewall log, router log, intrusion detection system log, application log, database log, etc.).

30) Audit trails should make it possible to:

(a) reconstruct events;

(b) establish responsibility for operations performed on the information system;

(c) detect unauthorised access to and operations performed on the information system;

(d) identify problems.

31) *A malicious code* is any type of code created with the purpose of acting in an unexpected and potentially damaging way, i.e. in the way that can disrupt confidentiality, integrity and availability of information system resources. The examples of malicious code include worms, viruses and Trojan horses.

32) *Electronic banking* is a direct offer of new and traditional products and services to clients through electronic interactive communication channels.

33) *Electronic banking* includes systems that provide credit institution clients with banking products and services (e.g. access to financial information, information on products and services, electronic payment services).

34) *An incident* is any unexpected or undesired event that can disrupt the security and functioning of the information system resources which support the carrying out of a credit institution's business processes.

35) *Recovery time objective* is an acceptable period of the unavailability of a credit institution's business processes and of the information system resources necessary for their carrying out , i.e. the time required to restore (recover) the business processes.

36) *Critical and/or vital business processes* are the business processes identified as such by the credit institution, whose unavailability may seriously threaten or disrupt the credit institution's operation.

37) *Back-up data copies* are auxiliary versions of data (information assets and software components) required to restore (recover) the credit institution's business processes, and of other data which the credit institution determines as necessary to be stored as a backup.

3 FRAMEWORK FOR INFORMATION SYSTEM MANAGEMENT

Article 3

A credit institution's management board shall nominate a member of the management board responsible for the setting up and supervision of information system management.

Article 4

A credit institution's management board shall establish an appropriate organisational structure, set up the relevant functions and committees and, accordingly, delegate the authority in order to ensure adequate management of the credit institution's information system.

Article 5

(1) A credit institution's management board shall adopt an information system strategy, which has to comply with the credit institution's business strategy.

(2) A credit institution's information system strategy shall be elaborated by adopting strategic and operational plans.

Article 6

A credit institution's management board shall adopt internal bylaws governing the information system management and ensure their implementation.

Article 7

A credit institution's management board shall ensure that all information system users are acquainted with the contents of the internal bylaws relating to the information system, in accordance with their delegated authorities and needs of information system users.

Article 8

A credit institution shall define the criteria, methods and procedures for notifying the management and supervisory boards of the relevant facts pertaining to the functionality and security of the information system.

Article 9

A credit institution's management board shall set up the function of information system security manager, which shall be independent of the function of information technology unit manager, and shall define his/her authority, responsibilities and the scope of activity.

Article 10

A credit institution's management board shall appoint an information technology steering committee or other committees responsible for monitoring and supervising the information system and its operations, and for co-ordinating the initiatives related to the information system, concerning its alignment with the credit institution's business goals and business strategy.

Article 11

A credit institution's management board shall adopt a project management methodology defining the criteria, methods and procedures for information system-related project management.

4 INFORMATION SYSTEM RISK MANAGEMENT

Article 12

The general rules for the implementation and setting up of a risk management system in terms of the Credit Institutions Act and regulations adopted pursuant to that Act, shall also apply to the information system risk management.

5 CONTRACTUAL RELATIONSHIP MANAGEMENT

Article 13

A credit institution shall assess and reduce to an acceptable level the risks arising from contractual relationships with legal and natural persons whose activities are connected with the credit institution's information system.

Article 14

A credit institution shall ensure ongoing supervision of the manner and the quality of the provision of contractual services related to the credit institution's information system.

6 INTERNAL AUDIT

Article 15

(1) A credit institution shall adopt a risk-based information system audit methodology in accordance with Article 187, paragraph (5) of the Credit Institutions Act which shall define the criteria, methods and procedures for the credit institution's information system auditing.

(2) The information system internal audit shall be subject to the provisions of the Decision on internal control systems (Official Gazette 1/2009, 75/2009 and 2/2010).

7 INFORMATION SYSTEM SECURITY

Article 16

A credit institution shall adopt an internal bylaw that will act as a framework for information system security management (hereinafter: information system security policy), and define responsibilities relating to the information system security.

Article 17

A credit institution shall classify and protect information according to its sensitivity with respect to the potential effects of disrupting the confidentiality, integrity and availability of information.

Article 18

A credit institution shall control the access to the information system resources, premises where the information system resources are located and the resources supporting the functioning of the information system and apply the appropriate administrative, logical and physical access controls. Special attention should be given to administrative and remote access to the information system resources.

Article 19

A credit institution shall establish the system of user access rights management, comprising the enrolment, authorisation, identification, authentication and supervision of user access rights.

Article 20

A credit institution shall, in accordance with the assessed risk, ensure the keeping of, and establish a retention period for audit trails (logs) which will make it possible to reconstruct events, establish responsibility for operations performed on the information system, detect unauthorised access to and operations performed on the information system and identify problems

Article 21

A credit institution shall protect its information system resources from a malicious code by implementing the appropriate administrative, logical and physical controls.

8 INFORMATION SYSTEM MAINTENANCE

Article 22

(1) A credit institution shall set up the process of the information system's hardware asset management during the life cycle of the assets.

(2) The hardware asset management process shall comprise the procedures for the detection, recording, disposing, monitoring, recovery and discarding of the assets.

Article 23

(1) A credit institution shall set up the process of managing the changes in the information system's software components, which shall comprise at least the following procedures:

(a) determining the initial versions of the information system's software components;

(b) identifying and monitoring any program changes in the application software that supports the provision of banking and financial services;

(c) identifying and monitoring any changes in the architecture of databases that support the provision of banking and financial services, and;

(d) identifying and monitoring the changes in any other information system's software components, which affect, or may affect, the functionality and/or security of the information system.

(2) Changes in the information system's software components shall be recorded and documented in order of occurrence, together with the time of their occurrence.

(3) All changes in the information system's software components shall be adequately tested and approved before implementation.

Article 24

A credit institution shall determine the procedures for creating, storing, maintaining and keeping the documentation related to the information system, and shall ensure that the documentation is accurate, complete and up-to-date.

Article 25

A credit institution shall provide for adequate and ongoing training of all the employees of a credit institution that use the information system.

9 BUSINESS CONTINUITY MANAGEMENT

Article 26

The process of business continuity management shall be subject to the provisions of the Decision on risk management (Official Gazette 1/2009, 41/2009, 75/2009, and 2/2010), unless otherwise prescribed by this Decision.

Article 27

In addition to the obligations prescribed by the Decision on risk management, in the context of business continuity management, a credit institution shall:

(a) adopt disaster recovery plan(s) providing for the recovery and availability of information system resources necessary for the carrying out of critical and/or vital business processes within the required time frame;

(b) periodically, and following significant changes in the business processes or the information system, perform appropriate disaster recovery plan testing and prepare written reports on the testing results.

Article 28

A credit institution shall set up an incident management process to ensure a timely and effective response in the event of violation of security and functionality of the information system resources supporting the carrying out of the business processes.

Article 29

In the event of major incidents, a credit institution shall, within an appropriate time frame from the occurrence of the incident, notify the Croatian National Bank of the incident, its effects and the actions taken.

Article 30

(1) A credit institution shall set up a backup storage management process, which shall comprise the procedures for making, storing and testing backup data copies, and for restoring data from the backup data copies in order to ensure data availability in the case of need, and to provide for the recovery or restoration of critical and/or vital business processes within the required time frame.

(2) The backup data copies must be up-to-date and stored in an appropriate manner at one or more locations of which at least one must be sufficiently far, in accordance with the assessed risk, from the location at which the source data (used for making the backup data copies) are held.

Article 31

A credit institution shall, in accordance with the assessed risk and the assessed impact of the unavailability of individual processes or information system resources necessary for carrying out such processes on the business of the credit institution, make available a backup computer centre with adequate equipment, functions and security level, which shall be located at an adequate distance from the primary computer centre.

10 INFORMATION SYSTEM DEVELOPMENT

Article 32

A credit institution shall define the methods, criteria and procedures for information system development, taking into account the functional and security aspects.

Article 33

A credit institution shall set up an information system development process in accordance with the adopted project management methodology.

Article 34

A credit institution shall, within its internal process of information system development, set up and document a process of software development and information system delivery which shall comprise the procedures for analysis and design, programming, testing and bringing into production.

Article 35

A credit institution shall ensure that all the developed information system software components, as well as new information system hardware components are adequately tested and approved before being brought into production.

Article 36

A credit institution shall appropriately separate the development, testing and production environments.

11 ELECTRONIC BANKING

Article 37

(1) A credit institution shall apply secure and efficient authentication methods to verify the identity and authority of persons, processes and systems.

(2) Wherever possible, authentication of persons must include a combination of at least two ways of user identity verification.

Article 38

A credit institution shall provide adequate verification of its identity in the electronic banking distribution channel, to ensure that electronic banking users can verify the identity and authenticity of the credit institution.

Article 39

A credit institution shall provide for adequate audit trails (logs) to ensure non-repudiation and verifiability of activities related to electronic banking.

12 TRANSITIONAL AND FINAL PROVISIONS

Article 40

As of the date of entry into force of this Decision, the Decision on adequate information system management (Official Gazette 80/2007) shall cease to have effect.

Article 41

This Decision shall be published in the Official Gazette and shall enter into force on 31 March 2010, with the exception of Article 23, paragraph (1), Article 26, Article 27, Article 30, paragraph (1) and Article 31 that shall enter into force on 1 July 2010.

Dec. No. 139-020/03-10/ŽR

Zagreb, 17 March 2010

Croatian National Bank
Governor
Željko Rohatinski