R E P U B L I C O F A L B A N I A
B A N K O F A L B A N I A
SUPERVISORY COUNCIL

REGULATION

"ON THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGY IN THE ENTITIES BEING GRANTED A LICENSE FROM THE BANK OF ALBANIA"

Approved with decision of Supervisory Council of Bank of Albania no.32, dated 03.05.2006.

Article1
Legal ground

This regulation is issued for the implementation of the Law No. 8269 dated 23.12.1997 "On the Bank of Albania" and the Law No. 8365 dated 02.07.1998 "On the Banking System in the Republic of Albania".

Article 2
Scope

(1) This regulation shall establish the criteria and conditions that the entities of this regulation have to complete on the organisation and functioning of their Information and Communication Technology systems (following referred as ICT).

(2) The definition of these criteria and conditions on the organisation and functioning of ICT systems and their implementation, aims to reduce the operational risk that might be arose from the misuse of ICT systems, and to provide the reliability of these systems in supporting the activity of these entities.

Article 3
Subjects

(1) Subject to this regulation (hereinafter refereed as entity) are:

a. banks and branches of foreign banks that conduct banking activity in the Republic of Albania, excluding the Bank of Albania;
b. Non-banking financial institutions and the Savings-loans associations;

(2) Notwithstanding paragraph (1) of this article, Bank of Albania shall verify the implementation of all the requirements, being provided in this regulation, even for the other entities being reasonably granted a license from the Bank of Albania, and depending on their activity size and complexity and of their ICT systems.

Article 4
Planning and organisation of the procedures

(1) The entity shall set up the targets, strategies and the security requirements on the activity of the respective ICT systems. The Executive Board, assigned by the entity or any other authorised structure, shall adopt the procedures relevant to each process on the management, operation, protection of the systems and on the preservation of the data as well as the procedures on the expulsion of these data.

(2) If the entity provides the whole or part of its ICT activity (or of its systems) by the external service suppliers, then the entity shall perform and adopt procedures and guidelines, which ensure the compliance with the requirements, as stated in this regulation on the security and well - functioning of these systems.

(3) The entity shall assign an internal officer, specialised in the information technology field, as a responsible for different aspects of the TCI activity.

Article 5
Risk analyses

(1) The entity shall set up the criteria on the allowed risk related to the use of its relevant ICT systems; it shall determine the responsible functions on their implementation and monitoring; and it shall conduct regularly analyses of this risk.

(2) At least once a year or in any event of key changes occurring in the TCI security requirements, the entity shall conducts risk analyses to ensure this risk is maintained within the accepted limits related to the entity activity. The outcomes from the risk analyses must be documented.

Article 6
The establishment of qualitative targets

(1) On each aspect of its ICT activity, the entity shall establish qualitative targets, which must be in compliance with the other objectives. These targets reflect the entity's expectations on the outcomes and services quality that arises or became possible by its ICT systems. The entity conducts periodic reviews on the compatibility and completeness of these targets and documents the related findings.

(2) In the implementation of paragraph (1) of this article, the targets on the products and services' quality deriving out or which are made possible by the ICT systems that the entity employs, should minimally comprise the requests on information security, being stored in the ICT systems, on the data reliability and their production in due time and in an adequate manner.

Article 7
Maintenance and security in making use of the ICT systems

(1) The entity takes measures to ensure that its ICT systems are adequately maintained and managed to provide the stable and expected operation (the well-known one).

(2) In accordance with paragraph (1) of this article, the entity adopts and applies procedures to provide the well-using of its ICT systems and to protect them from any possible destroying event. These procedures shall contain tangible and verifiable definitions.

(3) The procedures on the use of the systems shall include the requirements on the protection of the equipments, of the systems and of the key data against damage, misuse, logical miss-functioning of the software and against the unauthorised use. These requirements must refer to and be consistent with the best practices of the related field.

(4) The processes on the protection of data from any event of destroy, shall include the requirements on their periodic and mandatory preservation in instruments and/or in systems and/or in information technology premises, which are different of those being employed to support the direct and daily activity of the entity.

(5) The above procedures include also guidelines on the definition, amendment, transfer and control of the authorisation to use the ICT systems.

Article 8
Development and procurement of ICT systems

(1) The entity shall adopt internal acts on the way of how it conducts the developments, changes and tests in its ICT systems. The ICT systems shall be placed in the normal operation, upon the documented approval of the specialised

employee (Security officer), who verifies the implementation of the procedures and of the well-functioning of the systems.

Article 9
Dealing with deviations (miss-functioning) and changes

(1) The entity shall adopt procedures on dealing with the deviations and changes occurring in its relevant ICT systems, and ensures the compatibility with their requirements. The operations being taken for the purpose of these procedures shall be documented and saved as well.

(2) The procedures on dealing with the deviations include any miss-functioning, which arises from the operation of ICT systems. The reestablishment of the normal conditions on the functioning of its ICT systems is subject to these procedures. The process of dealing with these deviations shall include the identification of their cause, the prevention of recurrences as well as it provides for the adequate and transparent process of dealing with them. The deviations and the relevant correcting measures shall be documented. The procedures on dealing with the deviations shall contain guidelines on the escalation of the operations according to both the type of the deviation and the responsible function.

(3) The procedures, on dealing with the performed amendment, set up the criteria on dealing with any amendment, which impacts the production system of data. These procedures require the adequate and transparent treatment as well as the documentation of these changes. The entity shall provide that the procedures on dealing with the occurred change should make possible a stable and expected operation of its ICT systems.

Article 10
The continuing operation of ICT systems

(1) The entity shall adopt a contingency plan related to the operation of its ICT systems. In the framework of this plan, there are compiled procedures where there are determined the potential risks as well as the way of operating, the roles and responsibilities of the respective assigned structures and persons. The entity, having regard to the risk analyses, in accordance with article 5 of this regulation, shall identify its ICT systems pursuant to the importance degree, which must be included in the contingency plan.

(2) The entity, previously in the contingency plan:

a. shall identify and evaluate specific elements of ICT systems that may fail and preview an adequate response (reaction);
b. shall set up the criteria related to the selection of the back –up solutions;
c. shall set up the recovering procedures;

d. shall determine the guidelines to inform the managers, employees, and as it is the case the clients and service providers;

(3) The entity shall take the measures to conduct at a adequate degree the training of the relevant staff, the back-up exercising and tests, to provide the required reliability these solutions act in a satisfaction way. The tests shall be documented in a way their implementation and results be assessed in the future, in line with the internal needs and policies of the entity.

Article 11
The preparation on the disruption of the operations due to extraordinary events

(1) The entity shall adopt, in a documented way, a contingency plan related to extraordinary events, due to which the ICT operations could not continue based on the common resources, as being expected and enforced.

(2)The recovery plan, in case of extraordinary events, shall contain minimally:

a. a summary of the ICT systems, to be recovered;
b. a description of the contingency plan and of the measures it contains;
c. clearly established criteria on the operation of the contingency plan;
d. the procedures, which determine the necessary operations on recovering the ICT systems;
f. a general description of all the responsibilities and procedures upon making active the recovering plan;
g. the guidelines to inform the employees being impacted from the extraordinary event, pursuant to the case and need; to inform the service suppliers, the customers, the public authorities and the media.

(3) The entity shall perform once a year, trainings, exercises and tests in a degree to create the reliability that the recovering plan in any extraordinary event is acting as being previewed therein. The results shall be accurately documented, to be assessed in the future pursuant to the entity needs.

Article 12
Providing the service from the external suppliers

(1) The entity is accountable to ensure its respective ICT activity is performed in line with all the requests being established in this regulation, and with the other ones related to this activity. This request is applicable also even in case the entire or part of ICT activity is provided from other parties (external service provider). In this case, it is signed an agreement, in written form, between the entity and the external service supplier, providing the right to the entity to examine and control the activity of ICT external service provider, as it is stated in

the agreement. The agreement shall include clear definitions on the dealing with and preservation of the confidential information.

(2) The agreement, as laid down in paragraph (1) of this article, contains the definition that the Bank of Albania is vested with the right to know the information the entity provides from the external supplier of the ICT service, and/or with the external auditor reports of the external service supplier.

(3) The entity, pursuant to the requirements or through the official collaboration with the other parties, which do not represent the external ICT service, shall become ensure to have the required ability to manage the agreement as determined in paragraph (1) of this article.

Article 13
Documentation

The entity maintains a full and updated documentation on the organization, equipments, on the systems and on the other critical factors which are related with its CT activity. Such documentation shall prove that the compliance with the requirements of this regulation occurs on continuous basis.

Article 14
Complementary Materials

(1) To conduct the analysis on the implementation of these regulation requirements there shall be employed as follows:

1. the questionnaire to assess the ICT activity;
2. the questionnaire on the contingency plan in any case of extraordinary events.

(2) The questionnaires as established in paragraph (1) of this article, shall be delivered to the entities being provided in this regulation from the Banking Supervision Department of the Bank of Albania at the beginning of the examination and shall be completed by the entities having regard to the way and time as determined from the Banking Supervision Department. If required from the Banking Supervision Department, the questionnaires responses are followed by the respective certified documentation as being provided from the entity.

Article 15
Maintenance of the documentation

The entity shall keep the originated documentation according to the requirements of this regulation; pursuant to:

a) the general and specific legal and regulative requirements on dealing with the documentation, where the entity is subject;
b) the needs or internal requirements on the documentation.

Article 16
Corrective measures and penalties

In any event of violation of the requirements found in this regulation, there shall be implemented all the corrective measures and penalties, as laid down in article 44 of the Law No.8268 " On the Banking System in the Republic of Albania" and the bylaws issued by the Bank of Albania in the implementation of this law.

Article 17
Entry into Force

(1) Upon the approval of this regulation, its requirements composes the terms on granting a licenses to the entities, and form part of the overall evaluation process of the entity performed from the Banking Supervision Department of the Bank of Albania.

(2) Upon the approval of the Supervisory Council of the Bank of Albania, the requirements found in this regulation must be implemented from the entity applying for the first time to be granted an operational license.

(3) Having regard to the actual entities, the requirements of this regulation must be completed within January 1st, 2007.

(4) The Banking Supervision Department of the Bank of Albania shall compile and adopt the manual on the Inspection of Information and Communication Technology systems, within 90 days from the date of this regulation approval.

(5) This regulation shall enter into force upon the approval from the Supervisory Council of the Bank of Albania.

CHAIRMAN OF THE SUPERVISORY COUNCIL

Ardian Fullani