Pursuant to Article 17, paragraph 1, point 2 of the Law on Central Bank of Montenegro ("OGRM" 52/00 and 47/01) and Article 64, paragraph 3 of the Law on Banks ("OGRM" 52/00 and 32/02), the Council of the Central Bank of Montenegro, at the meeting held on 23 and 24 February 2009, enacted,

D E C I S I O N
On Minimum Standards for Operational Risk Management in Banks

1. General Provision

Subject Matter of Regulation

Article 1

This Decision shall govern minimum standards for managing operational risk in banks.

2. Operational Risk Management

Identification of Sources of Operational Risk

Article 2

In the procedure of identifying sources of operational risk, the bank shall identify, in particular, the risks arising from:

1) inadequate information and other systems in the bank;
2) disruptions in operations or system breakdown, such as defects of hardware or software, telecommunication problems or interruptions in the work of equipment, etc;
3) failure in ensuring adequate integration or sustainability of information and other systems, in case of status changes of the bank;
4) illegal and inadequate actions by bank employees, such as fraud, money laundering, unauthorized approach to client accounts, misuse of confidential client information, giving false or incorrect information about the bank positions, imprecision in performing the operations, errors in data inputs and non-observance of good business practices, etc;
5) recruting external persons for performing operations for the bank;
6) acts or omissions that may result in court or other lawsuits against a bank (legal risk);

7) external illegal actions, such as theft, unauthorized transfer of funds, forgery, unauthorized access to databases and illegal asquisition of bank's documents, etc;
8) unpredictable events such as natural and other disasters, terrorism, etc.

Measurement and Control of Risk

Article 3

A bank shall evaluate level of risk applying adequate measurement methods after identification of actual source of operational risk.

Subject to the nature and level of operational risk, the bank shall choose appropriate methods for its reduction or elimination, or for its monitoring and control.

A bank, which calculates required capital for the operational risk by applying the standardised method, shall monitor and measure the operational risk in all operational areas.

Identification of New Sources of Risk

Article 4

Before introducing new products, processes and systems, or before undertaking new business activities, the bank shall identify and assess the operational risk associated with them.

Definition of Powers and Responsibilities

Article 5

A bank shall clearly define in its rules and regulations powers and responsibilities for operational risk management.

A bank shall provide that all employees are familiar with their obligations in operational risk management process.

Internal Reporting

Article 6

The bank shall prescribe an obligation and methods of adequate internal reporting and periodic review of the operational risk management system in its rules and regulations.

Information System of a Bank as a Source of the Operational Risk

Article 7

Subject to providing adequate operational risk management arising from information system, a bank, as a minimum, shall:

1) establish information system strategy which shall be adjusted to the business strategy of a bank;
2) enact internal regulation as a frame for information system security management, which shall ensure:
   - classification and protection of information according to the degree of their sensitivity, bearing in mind possible consequences of infringement of confidentiality, integrity and information availability;
   - control of the approach to the information system resources, its premises and systems serving as a support to the information system functioning and implementation of corresponding managerial, logical and physical controls of the approach;
   - establishment of the system for managing user rights including processes of recording, authorization, identifications, authentication and oversight of user rights;
   - protection of non-material information system resources from malicious program code by implementation of corresponding managerial, logical and physical controls;
   - creation and protection of operational and system recordings which shall enable reconstruction of the event, disclosure of unauthorized approaches and operations on the information system, identification of a problem and determination of responsibility;
   - establishment of process of incident management which shall enable timely and efficient response in case of infringement of safety and functionality of the information system resources acting as support to business processes;
   - corresponding testing and approval of advanced information system software components and new hardware components, prior to their involvement in operations.

The Central Bank of Montenegro (hereinafter: the Central Bank) may create instructions for implementation of provisions from the paragraph 1 of this Article.

E-banking as a Source of the Operational Risk

Article 8

Subject to the control of the operational risk arising from e-banking services, a bank which offers e-banking services, as a minimum, shall:

1) implement safe and efficient mechanisms as a confirmation of authenticity and authorization of persons, processes and systems;
2) provide corresponding confirmation of its identity on the e-banking distribution channel, thus enabling e-banking users to check bank's identity;

3) secure existence of corresponding operational and system recordings which undisputedly confirm actions related to e-banking.

Data Protection

Article 9

A bank shall establish process of backup data copies management. This process shall include creation, keeping and testing of backup data copies so as to secure availability of data in case of necessity and to enable recovery, that is, reestablishment of vital business processes within the required time frame.

Backup data copies shall be updated and kept in a proper manner at one or more backup locations of which at least one must be, according to the risk assessment, distant enough from the location of original data.

Contingency Planning

Article 10

The bank shall make a contingency plan, in order to provide continued operation in case of serious disruptions of work caused by reasons that are beyond the bank's control.

The plan referred to in paragraph 1 shall determine:

1) the key business activities where continuity must be maintained even in emergency circumstances;
2) scenarios that might cause interruption of key business processes in the bank;
3) alternative solutions for maintaining continuity in the performance of key business activities in extraordinary circumstances;
4) activities for establishing regular functioning of operations, especially for ensuring recovery of information system which shall enable recovery and availability of information system resources needed for performance of key business processes within the required time frame;

The bank shall test the plan referred to in paragraph 1 above at least once a year and the test results shall be presented to the management board.

Register of Losses

Article 11

The bank shall establish a database on all incurred losses related to operational risk and methodology for internal recording of those losses under categories determined based on sources of losses.

A bank, which uses standardized method for the calculation of required capital for the operational risk, shall arrange data on losses arising from operational risk according to

corresponding business areas and according to categories established on the basis of the sources of losses.

Reporting to the Central Bank

Article 12

The bank shall inform the Central Bank on any losses arising from operational risk exceeding 1% bank's own funds, latest within eight days as of the day of incurring the loss.

The report referred to in paragraph 2 of this Article shall include causes and amount of the loss, the actions undertaken by the bank to recover the loss, and the actions that the bank has undertaken or intends to undertake in order to prevent similar losses happening in the future.

3. Closing Provisions

Article 13

Decision on Minimum Standards for Operational Risk Management in Banks ("OGRM". 08/05) shall cease to be valid as of the day this Decision enters into force.

Article 14

This Decision shall entry into force on the eighth day following its publication in the Official Gazette of the Republic of Montenegro, except Articles 7 and 8 whcih shall come into force on 1 January 2010.

THE COUNCIL OF THE CENTRAL BANK OF MONTENEGRO

PRESIDENT

Ljubiša Krgovic

Decision No. 0101-325/2-29
Podgorica, 24 February .2009