REPUBIC OF ALBANIA
BANK OF ALBANIA
SUPERVISIORY COUNCIL

DECISION
No. 03, dated 19.01. 2011

THE APPROVAL OF REGULATION
“ON THE OPERATIONAL RISK MANAGEMENT”

In accordance with Article 12 “a” and Article 43 “c” of the Law No. 8269, dated 23.12.1997 “On the Bank of Albania” as amended; and Article 57, paragraph 4 and Article 58, paragraph 1 “c” and Article 126 of the Law No. 9662, dated 18.12.2006 “On Banks in the Republic of Albania”; and Article 46 and Article 47, paragraph 2 of the Law No. 8782, dated 03.05.2001 “On Savings and Credit Associations”, as amended; having regard to the proposal from Supervision Department, the Supervisory Council of the Bank of Albania,

DECIDED:

1. To adopt the Regulation “On the operational risk management” and its annexes, as provided in the texture attached thereto.

2. The Supervision Department at the Bank of Albania is responsible for the implementation of this Decision.

3. The Department of Foreign Relations, European Integration and Communication is responsible for the publication of this Decision in the Official Bulletin of the Bank of Albania and in the Official Journal of the Republic of Albania.

This Decision shall enter into force on the 15th day following that of its publication in the Official Journal of the Republic of Albania.

SECRETARY	**CHAIRMAN**
YLLI MEMISHA	**ARDIAN FULLANI**

REGULATION

"ON THE OPERATIONAL RISK MANAGEMENT"

Chapter I
General provisions

Article 1
Purpose

This Regulation shall set out the requirements and rules for the operational risk management in the banking and/or financial activity from the subjects of this Regulation.

Article 2
Legal ground

This regulation is issued in accordance with:

a) Article 12 "a" and Article 43 "c" of the Law No. 8269 dated 23.12.1997 "On the Bank of Albania", as amended;
b) Article 57, paragraph 4 and Article 58, paragraph 1 "c" and Article 126 of the Law No. 9662, dated 18.12.2006 "On Banks in the Republic of Albania", which shall be referred as the "Law on Banks" throughout in this Regulation;
c) Article 46 and Article 47, paragraph 2 of the Law No. 8782 dated 03.05.2001 "On Savings and Credit Associations", as amended.

Article 3
Subjects

This Regulation shall apply on banks and branches of foreign banks, the non-bank financial institutions and the savings and credit associations and their unions, being granted a license from the Bank of Albania, to conduct banking and financial activity in the Republic of Albania.

Article 4
Definitions

1. The terms used throughout in this Regulation shall have the same meanings with those set forth in the Law on Banks and in the Law No. 8782 dated 03.05.2001 "On Savings and Credit Associations", as amended.

2. The terms used in this Regulation, “Steering Council” and “Directorate”, which refer to the legal organisation from of banks, neither restrict nor limit the implementation of this Regulation’s requirements for the other entities. These terms in case of other entities, which are not organised as banks, shall imply the respective authorities of entities, which carry out the analogue functions of the “Steering Council” and “Directorate”, depending on their legal organisation.

3. In addition to paragraph 1 of this Article, for the purpose of implementing this Regulation, the following terms shall have these meanings:

    a) “operational risk” – is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This definition includes legal risk, but excludes reputational and strategic risk. For the purposes of the internal operational risk management system, the entities may set out more specific definitions of this risk, with the condition these latter minimally incorporate the elements of this regulation definition;
    b) “legal risk” – shall imply the potential for financial loss arising from the failure of implementing or the incorrect implementation of the legal an/or contractual obligations, including other legal procedures which may negatively impact the financial outcome arising financial loss risk for the activity of entities;
    c) “strategic risk” – shall imply the potential for financial loss arising from the improper strategic decision in the business of the entities;
    d) “reputational risk” – shall imply the potential for financial loss arising from the decreasing of reputation in the entity/entities activity due to the negative perception on the part of public to the entity/entities.

Chapter II
General requirements for the operational risk management

Article 5
Operational Risk Management System

1. The entities of this Regulation, notwithstanding the size and complexity of their organisation and activity, shall establish and develop an adequate internal system (policies, procedures, guidelines and techniques) on the operational risk management. The purpose of this system is to identify, assess, control and monitor the comprehensive operational risk on an ongoing basis.

2. The operational risk management system of the institution should minimally include the following elements:

a) the identification, with regard to/depending on the entity's activity size, of the operational risk at the entity;
b) the comprehensiveness of the expected events which may arise material operational risks to the entity (including those set forth in Annex 1 of this Regulation);
c) the policies to identify, assess, monitor and control or mitigate this risk, including and specifying (whenever possible) the allowed limits of the operational risk;
d) the more prior actions for the entity in the management process of operational risk, also including the scale and the transfer way of this risk out from the entity.

Article 6
Responsibilities of the Steering Council

1. The Steering Council is the responsible authority for the establishment and development of the operational risk management system, as stipulated in Article 5 of this Regulation.

2. The Steering Council, in the framework of the operational risk management, is responsible for:

   a) the approval of respective policies and procedures for the operational risk management;
   b) the establishment of a management unit, able to implement the internal regulatory acts of the entity for the operational risk management;
   c) the clear assignment of responsibilities segregation and the reporting lines among the functions of the operational risk control, the business lines and the supporting functions;
   d) the regular review of the entity regulatory acts for the operational risk management with the purpose the operational risks management arising from the external market and other factors, as well as those operational risks associated with new products, activities or systems. The reviewing process should aim the assessment and the selection of the best operational risk management practices, appropriate with the entity's businesses, systems and processes.

3. The Steering Council shall ensure that the system for the operational risk management goes through an effective and comprehensive internal control process by an independent, qualified and responsible staff.

Article 7
Responsibilities of the Directorate

1. The Directorate is responsible for the implementation of the internal regulatory acts for managing the entity operational risk, as adopted by the Steering Council.

2. The Directorate, for the purpose of the operational risk management, shall be responsible for:

   a) the implementation of policies, procedures and processes for managing operational risk in all services/products, businesses and systems which are important for the entity;
   b) the ongoing implementation of all the internal bylaws for the operational risk management from all the entity structures;
   c) the implementation of responsibilities and the development of reporting lines, to encourage and maintain the accountability, to provide the needed financial and human resources for effective managing of the operational risk;
   d) clear communication of the entity's policy for the operational risk management to the employee of all levels, particularly in the units exposed to the operational risk;
   e) the conduction of bank and/or financial activities of the entity by a qualified staff with the necessary experience and technical capabilities;
   f) the ensuring that staff, responsible for monitoring the implementation of operational risk management policy, is independent from the units they oversee;
   g) the providing of the policies, processes and procedures documentation related to the advanced technologies, which in particular support the high amount transactions.

Chapter III
Operational Risk Management

Article 8
The identification and assessment of the operational risk

1. The entities shall identify and assess the operational risk in all material services/products, activities, processes and systems.

2. The entities, prior to the launch into the market of the new services/products, the conduction of various operations or processes, and/or the establishment of new systems, shall ensure the implementation of the appropriate and sufficient procedures for the prior assessment of the relevant operational risk.

3. The entities shall effectively identify the operational risk by considering both internal factors (as: entity structure, the activities nature, the quality of human resource, the organisational changes and the circulation of employees) and external factors (as: changes in the industry and technology advancements), which may unfavourably impact the achievement of the entity's objectives.

4. The entities shall assess their exposure to identified risks, thus defining their risk profile with the purpose the efficient use of human and technical resources for the management of these risks.

5. The entities shall set forth their methods and techniques to identify and asses the operational risk. Annex 2, attached to this Regulation, sets out some of the methods that the entities may employ to detect and assess the operational risk.

Article 9
The monitoring and reporting of the operational risk

1. The entities shall develop a regular monitoring and reporting process of the operational risk and the exposure against this risk to quickly identify and advance the shortfalls in risk management policies, procedures and practices.

2. The entities, in conducting the ongoing and effective monitoring process of the operational risk, shall:

   a) set out adequate indicators to ensure the early warning of the operational risk increase, which may arise losses in the future;
   b) set out limits on these indicators, whenever possible, to establish an effective monitoring process, which may help to identify the main and important risks to the entity and to provide to this later the monitoring of these risks timely;
   c) set out the monitoring process periodicity, by considering the risk scale and the nature of changes in the environment they operate within;
   d) ensure the enclosure of the monitoring results within the regular reports submitted to the Directorate and to the Steering Council.

3. The entities shall implement internal procedures which ensure the regular reporting to the Directorate and to the Steering Council, respectively by business units, from the function/organisational unit of operational risk management and by the internal audit unit.

4. The operational risk reports, as stipulated in paragraph 3 of this Article, should contain the following:

   a) the data regarding the financial, the internal operational position and the observation of limits set out for the risk indicators, as well as the information on the market important changes to the decision-making;
   b) a complete statement on each identified problem and instructions for the correcting operations with regard to the unresolved issues.

5. The entities shall ensure the delivery of reports to all management levels and to the business lines representatives, which are affected by the problems reflected in the

Article 10
Control and mitigation of the operational risk

1. The entities shall compile and implement policies, procedures and practices to control and/or mitigate the material operational risks.

2. The entities, for the purpose of controlling and mitigating the operational risk, shall:

   a) design a system of controlling procedures and practices for ensuring compliance with operational risk management internal policies;
   b) establish an effective internal control system containing an appropriate segregation of duties;
   c) in addition to segregation of duties, entities should ensure that other internal practices/procedures are in place as appropriate to address operational risk, including:

      i. close monitoring of adherence to assigned risk limits or thresholds,
      ii. safeguards for access to, and use of, entities data and assets, including the insurance contracts,
      iii. appropriate staffing level and training to maintain expertise,
      iv. identification of business lines or products where returns appear to be out of line with reasonable expectations,
      v. termination of business line/lines with high potential exposure and loss arising from operational risk, and
      vi. regular verification and reconciliation of accounts and transactions;

   d) use tools or programs to lower the exposure to events with low probability, but which may considerably impact their financial result;
   e) pay special attention to the activities and/or the establishment of new products, particularly if these latter oppose their business plan;
   f) play special attention to the introduction into unknown markets and/or the commitment of trading activities, which are geographically conducted far from the head office;
   g) invest in the right use and the information technology security, providing the proper attention with regard to the strengthening of services automating degree;
   h) establish policies on risk management that arises from the transfer of functions and/or responsibilities of the entity to third parties.

3. The entities shall regularly review their policies and procedures for controlling and mitigating the operational risk, aiming the employment of adequate strategies

commensurate with their risk profile, as well as with the established circumstances and environment.

Article 11
Business Continuity Plan

1. The entities shall have business continuity plans in place, which aim the operation on an ongoing basis and limit losses related to operational risk.

2. The entities shall ensure that business continuity plans are integrated part of the operational risk management system and/or of other risks.

3. The entities, to design and approve these plans, shall identify:

   a) critical business operations, whose conduction should be ensured even under emergency situations;
   b) scenarios/events, which may lead to the disruption of processes and/or of the prior activities;
   c) alternative solutions to secure the continuing conduction of the main activities in emergency situations;
   d) operations to recover the regular functioning of the activities, particularly to secure the information of electronic systems and the return of these systems in functional position;
   e) communication strategies in case of serious problems and/or of operations disruption.

4. The entities should periodically analyse and/or review their business continuity plans to ensure their consistence with current operations activity and their business strategies.

Chapter IV
Reporting and supervision

Article 12
Reporting to the Bank of Albania

The entities shall report annually and quarterly the data to the Bank of Albania accordingly to Annexes 6 and 7 of this Regulation.

Article 13
Supervisory and penalising measures

The Bank of Albania, in case of failure to meet the obligations set forth in this Regulation, shall implement the supervisory and/or penalising measures stipulated in the Law on Banks and in the Law “On Savings and Credit Associations”.

Chapter V

Article 14
Transitory Provision

The subjects of this Regulation, shall meet all the requirements set forth in this Regulation, within 6 (six) months after the entry into force of this Regulation.

Article 15
Final provision

The annexes attached therein are an integral part of this Regulation.

CHAIRMAN OF SUPERVISORY COUNCIL

ARDIAN FULLANI

ANNEX 1

Operational risk events that may trigger significant losses

Type of event	Definition
Internal fraud	Internal fraud is related with the conduction of unauthorised activities, stealing and/or frauds which involve at least one employee of the entity. Some events, classified as internal frauds, are provided following: a) wrong and intentional reportings of the entity positions; b) conduction of unauthorised transactions of the entity; c) internal transactions (under the account of the entity employee); d) intentional destroy of the entity assets; e) theft, rubbery, grabbing, misappropriations within the entity; f) counterfeits; g) intentional fiscal evasion.
External fraud	External fraud refers to the frauds and/or theft conducted by a third-party outside the entity. This include, *inter alia*; a) theft and rubbery; b) forgery c) *hacking damage*; d) theft of information; e) etc.
Employment practices and workplace safety	This category refers to the events related with the employees' relationships, work place safety and discrimination. Samples that may bring about operational loss, include *inter alia*: a) compensation of employees' complaints (for example: discrimination situations, etc); b) the wrong (unfair) termination of employment contract/contracts; c) infringement of health and safety rules.
Clients, products and business practices of the	In this category, the operational losses derive from the failure to meet a client's obligation, or from the product nature and projection. Examples of these situations, include:

activities	a) fiduciary breaches; b) misuse of the client's confidential information; c) money laundering; d) products defects; e) account churning; f) human or automatic calculations errors; g) exceeding of exposure limits against the client.
Damage to physical assets	This category includes losses owing to the disaster and/or other actions, such are: a) natural disaster, including (earthquakes, fire, deluge, etc); b) terrorism; c) vandalism.
Business disruption and system failures	The situations of operational risk in this category include, *inter alia*: a) utility disruptions and software failures; b) telecommunication problems; c) services disruption; d) outdating of equipment.
Execution, delivery and processes management	This category includes risk situations related to the processing of transactions or to the management of processes and relationships with third parties. Examples of such situations, amongst other, shall include: a) shortfalls in communication; b) data entry errors (example: wrong data); c) failure to meet the terms and responsibilities; d) malfunction of modules/systems; e) accounting errors; f) reporting errors; g) legal documentation shortfalls; h) unauthorised entry in the client's account; i) disputes with the third parties; j) failure of services contracts with third parties in line with the agreed terms.

ANNEX 2

Common approaches and techniques for managing the operational risk from the entities mainly include:

1. Risk assessment. The entities assess their operations and activities against potential weakness of the operational risk. This process is a self assessment and frequently includes check lists, scorecards, and work meetings to identify the strong points and weakness of the operational risk environment.

2. *Risk Mapping.* In this process, different business units, organisational functions or the process course are categorised (mapped) by the type of risk. This process may identify the weaknesses in different fields and can help prioritise subsequent management actions.

3. Risk indicators. Risk indicators mainly are statistics, frequently financial ones, which may provide insight into an institution risk' position of the entities and should be periodically reviewed.

4. Measurement. A range of approaches are used to identify/measure the exposure rates to the operational risk. For example: historical data on the entities' activity performance may provide insight into the assessment of their exposure against the operational risk and the development of policies to mitigate and control this risk. The establishment of a system for the systematic overseeing and recording of frequencies, events severity and other important information on individual losses events, is an effective way to use this information. The entities may combine internal data of losses from outside, conduct analyses based on scenarios and factors of the risk assessment.

Annex 3

Principles on the data collection and documentation

With the purpose the collection and documentation of data for the operational risk losses, the entities implement the following requirements:

1. The entities should be able to mapping the historical data of internal losses by business lines and types of events. The losses mapping by business lines and events type is carried out by using objective and documented criteria.

2. The data about the internal losses of the bank should be comprehensive, in order to include all the important activities and exposures for the entity/entities. The entities should be able to justify that each excluded activity or exposure, either individually or even those in co-operation, would not have had a significant impact on the overall risk assessment. Appropriate minimum limits should be set forth to collect internal losses data.

3. The entities, in addition to the information on the gross losses amount, should collect information on any recovery of the gross losses amount, and a descriptive information about the event causes.

4. The entities for identifying the data on losses, which derive from an event in a function or particular activity, which involves more than one business line, should use specific criteria.

ANNEX 4

Business lines mapping

No.	Business lines	List of activities
1.	Corporate finance	• signing of financial instruments and/or the placement of the financial instruments on an unreturned commitment basis; • services related to the signing; • advisory service in the investment field; • advisory services on capital structure, business strategy and related aspects, also advisory services related to the merging and purchasing of associations (enterprises); • research and financial analysis on investments and other general advisory ways related with the financial instruments transactions.
2.	Treasury operations	• trading for its account; • Interbank markets brokerage; • receiving and transmission of orders related to one or more financial instruments; • execution of orders for the account of clients; • placement of financial instruments not on the basis of an unreturned commitment; • management of a multilateral system; • Operation of Multilateral Trading Facilities.
3.	Retail Brokerage	• receiving and transmission of orders related to one or more financial instruments; • execution of orders for the account of clients; • placement of financial instruments not on the basis of unreturned commitment.
4.	Commercial banking	• acceptance of deposits and other repayable funds; • lending; • leasing; • supply of guaranties and commitments.
5.	Retail banking	• acceptance of deposits and other repayable funds;

		• lending; • financial leasing; • supply of guaranties and commitments.
6.	Payment and settlement	• the service of payments and money (funds) transfer; • issuance and management of payment means.
7.	Agency service	• preservation and management of financial instruments for the account of clients, including the conservatorship and other relevant services, such as: cash or real guaranties (collateral) management.
8.	Asset management	• portfolio management; • *Managing of UCITS* • other assets management ways.

Annex 5

Principles (requirement) for business lines mapping

The institutions shall compile special policies and criteria for the mapping of the respective indicators for the business lines and operations within a standardised framework. The criteria should be reviewed and adopted to new activities or/and with regard to each change of the business and risks, that the entity undertakes. The principles on the business lines mapping, are:

1. All operations should be completely mapped/incorporated within the business lines stipulated in Annex 4.

2. Any activity, which could not be mapped easily in the framework of the business lines, but which construct a facilitating function for an activity included in this lines framework, should be included in that business lines it supports. The institutions should set forth objective criteria for the mapping of the activities, whenever the facilitating activity supports more than one business line.

3. If an activity may not be mapped within a special business line, the institution should use one of the business lines as operated in case of facilitating activity.

4. The mapping of activities within the business lines, for the purposes of the operational risk, should be in line with the categories used for the classification of assets accordingly to credit and markets risks.

5. The mapping process of activities by business lines should be subject of independent analysis of the internal audit.

ANNEX 6

OPERATIONAL RISK: GROSS LOSSES BY BUSINESS LINES AND TYPES OF EVENTS OVER THE LAST YEAR

Losses mapping by business lines		Type of event							Total Events type	Limits used for the data collection	
		Internal fraud	External fraud	Employment practice and workplace safety	Clients, products and business practices of the activities	Damage to physical assets	Business disruption and system failures	Execution, delivery and processes management		The lowest rate	The highest rate
		1	2	3	4	5	6	7	8	9	10
Corporate finances	Number of events										
	Total losses amount										
	Maximum loss										
Treasury Transactions	Number of events										
	Total losses amount										
	Maximum loss										
Retail brokerage	Number of events										
	Total losses amount										
	Maximum loss										
Commercial Banking	Number of events										
	Total losses amount										
	Maximum loss										
Retail banking	Number of events										
	Total losses amount										
	Maximum loss										
Payment and	Number of										

settlement	events										
	Total losses amount										
	Maximum loss										
Agency service	Number of events										
	Total losses amount										
	Maximum loss										
Total Business lines	Number of events										
	Total losses amount										
	Maximum loss										

Note: The institution shall not fill in the highlighted squares.

Regulatory guidelines, comments and references for the above table (Annex 6).

No	LABLE	Regulatory guidelines, comments and references
		COLUMNS
1-7	Definition of events types	Regulation ”On minimum operational risk management standards” Annex 1
8	Total events type	For each business line, figures are a simple aggregation (number of events and total loss amount) or the maximum (maximum loss) of data by event type. There is a special case for the data on some events and maximum loss for “ total business lines” (See the following note “number of events”
	Limits used on data collection	Regulation "On minimum operational risk managements standards” Annex 3, paragraph 2
9,10	Lowest rate / highest rate	Regulation "On minimum operational risk management standards” Annex 3, paragraph 2 If there is only one limit for each business line event, there should be filled in only the column: the lowest rate. If there are various limits that are used within the same business line, then should be filled in both columns.
		ROWS
	Definition of business lines	Regulation "On minimum operational risk management standards”, Annex 4
	Loss mapping with business lines	Regulation "On minimum operational risk management standards” Annex 3, paragraphs 2 and 2. The following information required for each business line should be reported accordingly to the used limits (see the above note “Used limits for the collection of data”)
	Number of events	Number of events recorded in each business line. If any event impacts some business lines, there should be reported on all those line where loss is identified upper a definite level. Also, the total number of events for “Total business lines” and “Total of events type” shall be lower than the aggregation of events by business lines, for those events of multilateral impact shall be considered as a solely one.
	Total loss amount	The aggregation of losses recorded in the database for each business line and by the case, classified by the type of event.
	Maximum loss	The maximum recorded loss by business line. In case of maximum loss for “Total business lines” and “Total events types”, those events impacting different business lines shall be considered as a solely one.
	Total business lines	For each type of event, the figures are: - Number of events upper the established rate by type of event for “total business lines”. This figure may be lower than the aggregation of events type by business lines, as these events of multilateral impact shall be considered as a solely one. - Total losses amount is the simple aggregation of total losses amount for each business line. - Maximum loss is the maximum loss upper the established rate for each type of event and for the total business lines.

ANNEX 7

Reporting form of the key operational risk indicators

Institution:
Position:
Responsible person:
Date of reporting:

No.	indicator	Value	Comments
1	Legal case-A		
2	Legal case -B		
3	Clients' complaints-A		
4	Clients' complaints -B		
5	Authorities' complaints-A		
6	Authorities' complaints -B		
7	Circulation of employees		
8	Failure/interruption of the bank basic program		
9	Doubtful operations with cards		
10	Spread in the cashiers' balance-sheet		
11	Spread in the cashiers' balance-sheet		

Details and explanations with regard to the above form (Annex 7):

Key risk indicator					
Nr	Name	Description	Type	Standard	Reporting frequency
1	Legal case-A	Number of legal cases against the bank from clients or other parties during the previous quarter. It includes legal processes and any legal operation undertaken against the bank that may be submitted to the court. The legal cases related to the bank efforts to recover the non-performing loans or human resources cases with employees, are excluded.	Client/Counterparty interaction	Counting	Quarterly
2	Legal case-B	Legal cases cost (set forth by indicator 1) against the bank from clients or other parties over the previous quarter. The legal cases related to the bank efforts to recover the non-performing loans or human resources cases with employees, are excluded.	Client/Counterparty interaction	Monetary value	Quarterly
3	Client's complaints-A	Number of official complaints against the bank from clients, groups of clients or the public, during the previous quarter. It includes all the complaints attained over the previous quarter being closed, rejected or opened at the end of the previous quarter. There are excluded the complaints related to the cases of Human Resources with the employees.	Client/Counterparty interaction	Counting	Quarterly
4	Client's complaints-B	Number of official complaints against the bank from clients, groups of clients or the public, still resulting opened at the end of the previous quarter. The complaints related to cases of Human Resources with employees, are excluded.	Client/Counterparty interaction	Counting	Quarterly

5	Authorities' complaints-A	Number of formal complaints against the bank by the public authorities (People Attorney, regulators, ministries, etc) during the previous quarter, which may be finalised or not with a penalty. Here are included all complaints received during the previous quarter (closed or open). The complaints related with Human Resources cases with the employees are excluded.	Client/Counterparty interaction	Counting	Quarterly
6	Authorities' complaints-B	Number of formal complaints against the bank by the public authorities (People Attorney, regulators, ministries, etc), which result still open during the previous quarter. The complaints related to Human Resources cases with employees are excluded.	Client/Counterparty interaction	Counting	Quarterly
7	Circulation of employees*	Percentage of employees' circulation of all categories since the beginning of year to the end of the previous quarter. Here are included both full time and part time employees. The internal parties acting as agents or contractors are excluded.	Persons	Percentage	Quarterly
8	Failure/Interruption of the bank main program	Duration stated as a percentage, of unplanned disruptions of the bank basic programs over the previous quarter (the work period is measured on 24 –hour basis).	Systems	Percentage	Quarterly
9	Doubtful transactions with cards	Percentage of cards reported as lost/stolen or under justified investigation due to relevant fraud reasons over the previous quarter, against the total number of cards issued from the bank for its clients. (All types of cards).	Systems	Percentage	Quarterly
10	Spreads in bank tellers' balance-sheet	Total number of bank tellers' spreads (deficits & suffixes) over the previous quarter.	Processing	Counting	Quarterly
11	Spread in bank tellers' balance-sheet	Total amount of bank tellers' spreads (deficits & suffixes) over the previous quarter.	Processing	Monetary value	Quarterly

*** C=L/(P)*100, (P)=(P0+P1)/2**

Ku:

C –circulation of employees;

L – number of employees left over the reporting period;

(P) – average number of employees over the reporting period;

P0 – number of employees at the beginning of the period;

P1 – number of employees at the end of the period.