NATIONAL BANK OF THE REPUBLIC OF MACEDONIA

FINANCIAL STABILITY, BANKING REGULATIONS AND METHODOLOGIES DEPARTMENT

SUPERVISORY CIRCULAR 10 - OPERATIONAL RISK MANAGEMENT

- July 2011 -

CONTENTS

1. INTRODUCTION 3

2. DEFINITION OF OPERATIONAL RISK 5

3. NEW CAPITAL ACCORD AND OPERATIONAL RISK 7

3.1 Basic Indicator Approach 8

3.2 Standardized approach 9

3.2.1 Alternative standardized approach 12

3.3 Advanced measurement approach 14

3.3.1 Internal data 15

3.3.2 External data 16

3.3.3 Scenario analyses 16

3.3.4 Business environment and internal control systems 16

3.3.5. Techniques for operational risk mitigation 17

3.3.6. Problems in the implementation of the advanced measurement approach 17

3.4. Partial implementation 18

4. OPERATIONAL RISK MANAGEMENT 20

4.1. Role of the bank bodies in the operational risk management 20

4.2. Operational risk identification 21

4.3. Assessment or measurement of the operational risk 22

4.4. Monitoring and reporting on the operational risk 23

4.1.1. Reporting system 24

4.5. Control and mitigation of the operational risk 24

4.6. Business continuity plan and contingency plan 26

5. OUTSOURCING 28

5.1. Defining of outsourcing 28

5.2. Outsourcing policy 28

5.3. Assessment of the outsourcing risk 29

5.4. Selection of outsourcing 29

5.5. Defining of the contents of the contract with the outsourcing provider 30

5.6. Bank's oversight of the outsourcing 31

REFERENCE 32

1. INTRODUCTION

The development of financial market and the launch of complex financial products, as well as the growing presence of information technology in the banks' day-to-day operations made outstanding contribution to the work promotion and efficiency, and simultaneously, lie behind the increase of the banks' risk profile. These factors trigger new bank risks, as follows:

- the use of highly automated technology could turn the risk of errors in the manual data processing into the system errors risk,
- the growth of e-banking increases the incidence of potential risks,
- the higher volume of status changes such as acquisition, merger and division creates the need for testing the sustainability of new integrated systems,
- the use of risk mitigation techniques (various collaterals, credit derivatives, asset settlement and securitization agreements) to optimize the market and credit risk exposures could induce other risks, such as the legal risk or partial risk transmission,
- the outsourcing and participation in settlement systems decrease the presence of some risks, but could in turn, trigger new bank risks.

All these risks constitute the **operational risk** and should be included in the process of its management. Operational risk management is not a new practice because the banks already undertake actions to prevent against fraud, to establish efficient internal control and to reduce transactions-related risks. In the past, the banks, in the operational risk management, almost always relied upon the internal control system established in each business line, with the support of internal audit. With the new activities and technologies, serious consideration is given to the establishment of a comprehensive operational risk management process, same as for the credit and market risk. The increasing frequency of losses arising from operational risk made the banks and supervisory officers focus on this risk and include it the overall risk management system.

The operational risk management system, established and accepted by the individual bank, depends on number of factors, including the bank's size, and the nature and features of its operations. In spite of these differences, efficient operational risk management of each bank include establishment of a culture for understanding the operational risk, clear segregation of duties of the bank's bodies and efficient internal control of the operational risk management. Operational risk management is the most successful in banks that nourish the high ethical standards at all levels.

Taking into account such significance of the operational risk, the National Bank of the Republic of Macedonia (hereinafter: the National Bank) developed a circular, discussing the basic features of the operational risk and the establishment of efficient management system. In the preparation of this circular, the National Bank took into account the existing risk management regulations, the standards and principles defined by the Basel Committee on Bank Supervision and the Committee of

European Banking Supervisors[1], as well as the experience of other countries and their supervisory authorities.

The **first part** of this circular discusses the method of defining the operational risk in the international practice and by international institutions. **The second part** presents the analysis of operational risk treatment in the Basel Capital Accord (Basel 2) and how it is included in the calculation of the capital requirement. **The third part** tackles the operational risk management, presenting the stages of this process and the role of the bank's bodies in the establishment and the use of efficient operational risk management system. **The last part** of this circular especially focuses on the importance of the establishment of an adequate system for selection and control of outsourced activities.

[1] In line with the reforms of the financial supervision in the European Union, since January 1, 2011, this Committee was renamed into European Banking Authority.

2. DEFINITION OF OPERATIONAL RISK

Banks have been facing operational risk since the inception of the banking industry. The first definitions for this risk, however, emerged in the last ten years. **Until recently, this risk was defined as any risk which is not credit, market or liquidity risk.** Moreover, the banks did not include this risk in the overall risk management activities, and usually responded in the aftermath. The banks treated any loss arising from errors, frauds, thefts or similar contingencies, as an operating expense, and as events that should be prevented only by establishing adequate internal control system. Such approach provides limited possibilities for prediction and prevention against enormous losses, as was the case of the failure of Barings Bank from England in 1995. In the period of disaster of the Barings Bank, some large international banks became proactive in the operational risk management.

In this period, the banks came with their own operational risk definitions. The differences among definitions arise primarily from the type and level of banks exposure to operational risk. The operational risk exposure of various banks depends on the nature and features of bank's operations. However, in spite of the differences among definitions, each definition starts with identification of events that could trigger significant losses in the bank's operations. In general, these losses could arise from the events of operational risk exposure (hereinafter: risk events), given below:

- internal fraud (deliberate false reporting of some items, thefts by employees, trade by employees for their account using internal information, corruption, misconduct),
- external fraud (theft, embezzlement, hacking),
- work practices and job security (payment of indemnifications to employees, violation of law standards for health and social welfare and job security, discrimination of employees),
- clients, products and business practices (abuse of client's personal data, inadequate trading for the bank's account, money laundering, breach of contractual liabilities),
- impairment of fixed assets (terrorism, vandalism, earthquakes, fires, floods),
- discontinuity of business processes and system errors (software and hardware errors, telecommunication troubleshoots, obsolescence of assets),
- process implementation, delivery and management (data entry errors, security errors, incomplete legal documentation, unauthorized access to accounts, disputes with third parties).

Taking into account the previous operational risk elements, the Basel Committee on Banking Supervision (hereinafter: Basel Committee) provides, within the New Capital Accord (Basel 2), a definition of the operational risk broadly accepted by myriad of supervisory authorities worldwide (particularly those who have applied or will apply the New Capital Accord). According to this definition, **operational risk is a risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.** This definition also includes the legal risk, but does not include the strategic and reputational risk[2].

[2] The manner in which the Basel Committee defined the operational risk is discussed, in more details, in the next section - New Capital Accord and Operational Risk.

The definition of Basel Committee has also been incorporated in the Decision on Risk Management (hereinafter: Decision) adopted by the National Bank Council, according to which **an operational risk is a risk of loss as a result of:**

- **inadequate or failed internal processes,**
- **inadequate personnel and inadequate or failed systems of the bank,**
- **external events.**

This definition does not prevent the banks to consider different definition of operational risk, if the scope of such definition includes the elements required by the National Bank. Operational risk also includes legal risk, risk of money laundering and financing of terrorism, information system risk and other similar risks, but does not include strategic and reputational risk.

Legal risk has been defined as a current or prospective risk to the bank's profit and own funds, caused by violation or non-adherence to the legal framework, agreements, prescribed practices, ethics standards, or as a result of misinterpretation of the regulations, rules, agreements and other legal documents. **Information system risk** is a risk of loss for the bank arising from losing, unauthorized utilization, or unavailability of the information, information assets and/or services the bank provides. **Risk of money laundering and financing of terrorism** is a risk for the bank to be involved, deliberately or unintentionally, in activities which, according to the existing regulations or international standards, are regarded as money laundering or financing of terrorism.

1. NEW CAPITAL ACCORD AND OPERATIONAL RISK

Taking into account the effect of the operational risk exposure on the banks' operations, the Basel Committee included this risk in the methodology for determining capital adequacy ratio, as defined in the Basel Capital Accord (Basel 2)[3]. Thus, except for the credit and market risks, as risks included in the capital framework even prior to the adoption of the new capital accord, the banks are also required to allocate certain amount of capital requirement for operational risk.

The Basel Capital Accord (hereinafter: Accord) defines the operational risk and specifies approaches applicable when determining the capital requirement for this risk.

As mentioned above, according to the Accord, operational risk includes legal risk, but does not include strategic and reputational risk. Legal risk includes at least the exposure to misdemeanor sanctions, fines and other penalties resulting from imposed supervisory measures or private charges. The Basel Committee's definition for operational risk does not include reputational and strategic risk since they are barely quantifiable, i.e. it is hard to determine the severity of banks' loss arising from these risks. Such decision of the Basel Committee does not hold the banks back from including these two risks in the definition of the operational risk, for their internal purposes for managing this risk.

Besides the operational risk definition, the Accord also offers three approaches (methods) for calculating operational risk capital charges:

- Basic Indicator Approach,
- Standardized Approach,
- Advanced Measurement Approach.

The three approaches differ in their complexity and application options. The basic indicator approach is a simple approach easily applicable to the banks' systems for determining the capital adequacy. On the other hand, the advanced measurement approach uses internal models for determining the capital requirement for operational risk. Application of this approach requires advanced operational risk

[3] International Convergence of Capital Measurement and Capital Standards – A Revised Framework Comprehensive Version, June 2006. The New Capital Accord defines the methodology for determining capital adequacy, i.e. the level of capital requirement for bank risks. The New Accord, which is an evolution of the existing capital accord (Basel I), puts the amount of capital requirement in closer relation with the bank's risk profile. The bank's capital requirement is, in fact, a function of two factors: risk profile and risk management techniques and methods used by the bank. The new capital accord relies on three pillars: minimum capital requirements (Pillar 1), supervisory review process (Pillar 2) and market discipline (Pillar 3). The first pillar specifies several approaches (options) for calculating the capital requirement for credit, market and operational risks. Banks and supervisory authorities apply the second pillar for other risks not included in the first pillar of the New Capital Accord (such as interest rate risk of the banking book, concentration risk, etc.). The purpose of the third pillar is to promote high level of banks' transparency, by disclosing data and information that help understand the risk management system and the amount of capital requirement allocated for those risks.

identification, monitoring and control systems, suitable for large and complex, internationally active banks or banking groups.

The application of any of these three approaches depends on the willingness of each bank to meet the criteria defined in the Accord, and on the national regulations for determining capital adequacy. The Accord gives discretion to each national supervisor to define approaches applicable by the banks in the country. The national supervisor makes this decision taking into account the features and the nature of the banking system in its country. Hence, the national supervisor could allow application of all or only one/several approaches in the process of determining the capital requirement for operational risk.

The National Bank decided to apply the new Basel Accord step by step, taking into account the features of the banking system of the Republic of Macedonia. The first stage includes development of a regulation that will allow application of standardized approaches for determining the capital requirement for credit, market and operational risk. Therefore, in February 2009[4], amendments to the existing methodology for determining the capital adequacy were adopted, which will become applicable on December 31, 2011. These amendments will allow the banks to determine the capital requirement for operational risk by applying one of the two offered approaches: basic indicator approach and standardized approach. The second stage that includes stipulation of the use of advanced measurement approaches is to start in 2013.

3.1 Basic Indicator Approach

Banks using the Basic Indicator Approach must hold capital for operational risk equal to the average over the previous three years of a fixed percentage (denoted alpha) of positive annual gross income, or:

$$K_{BI} = \frac{\sum (GI_{1..n} \times \alpha)}{n}$$, where:

K_{BI} - the capital charge under the basic indicator approach

GI- annual gross income

n - number of the previous three years for which gross income is positive

α - 15%, which is set by the Basel Committee

If the bank reported negative gross income in any of the previous three years, that year will not be included in the determination of capital requirement. Accordingly, that year will be included neither in the numerator nor in the denominator of the given formula. Thus, as a result of the negative gross income in

[4]The current methodology already allows using standardized approach for market risk assessment. The amendments to the methodology for determining capital adequacy are underway, which are to allow application of a standardized approach for determining capital requirement for credit risk. These amendments would start being applied on 31.12.2011.

all three years, the bank could be exempted from allocation of capital requirement for operational risk. To avoid such events, the national supervisor has the right (based on criteria included in the second pillar of the Accord - supervisory review process) to determine additional capital requirement. The national supervisor establishes this amount taking into account the banking system experience with losses arising from operational risk, the amount of capital requirement for this risk determined by other banks with similar size and features, the operational risk management system in place in the bank, etc.

Gross income is a sum of net interest income and net non-interest income, as specified by the accounting framework used in each country. The gross income does not include:

- allocated impairment/special reserve,
- operating expenses, including fees paid to outsourcing service providers[5],
- extraordinary and irregular incomes, as well as income derived from insurance

The Accord defines no special criteria for the banks to become eligible for using this approach for determining the capital requirement for operational risk.

3.2 Standardized approach

Standardized approach uses the gross income determined in consistence with the definition applied in the basic indicator approach, as a basis for calculation of capital requirement for operational risk. **This approach differs from the basic indicator approach in the banks' obligation to divide its activities in eight business lines, and to calculate the gross income for each of these lines.** The eight business lines have been established by the Basel Committee as follows: corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency services, asset management and retail brokerage. Review of activities suitable for each business line, according to the Accord, are given below:

Business line	Activity
Corporate finance	Mergers and acquisitions, underwriting, public debt finance, privatizations, securitization, research, syndications, consultations
Trading and sales	Trade in debt and equity instruments, foreign currencies and commodities on own behalf and for own account, money market intermediation, conclusion of repos, securities borrowing and lending, securities brokerage and corporate finance (if not included in the business line "retail brokerage")
Retail banking	Retail lending and deposits, credit cards and other retail banking services Private banking (lending and deposits, banking services, investment advice), financial leasing, issue of guarantees, backing guarantees and similar

[5] Include only expenses for services by bank's parent entity, bank's subordinate entity or subordinate entity of the bank's parent entity.

	instruments.
Commercial banking	Lending and deposits, real estate, export finance, trade finance, factoring, leasing, guarantees, bills of exchange, project finance, and other types of specialized lending[6]
Payment and settlement[7]	Payments and collections, funds transfer, clearing and settlement for clients' accounts, issuing and administering means of payments.
Agency services	Custodial and alike services
Asset management	Securities portfolio management and other types of asset management on client's behalf and account
Retail brokerage	Execution of orders for account of clients not being large corporations (not included in the business line of trading and sales)

The bank could define different business lines as long as such division includes all activities and risk events defined in the Accord. In this case, the bank can, at all times, redistribute its activities among business lines specified by the Accord.

The bank shall assign a business line to each activity, by applying the following principles:

- all bank's activities shall be covered in a comprehensive and mutually exclusive manner,
- all activities that support other activity (auxiliary activity) shall be allocatted to the business line of the basic activity. If the auxiliary activity is carried out to support several activities, the bank uses an objective-allocation criteria, and these criteria must be applied consistently in all similar cases,
- if the activity can not be allocated in any business line, it shall be allocated into a business line with the highest capital requirements ratio. This business line shall also be assigned to all auxiliary activities of such activity,
- the costs generated in one business line, simultaneously referring to other business line, may be allocated to adequate business lines according to internal allocation methods,
- the allocation process of individual activities into business lines must be fully documented. The bank is obliged to have clear and detailed definitions for each business line,
- the allocation of the activities into business lines and the manner of calculation of the gross income shall be subject to independent review by the internal audit department or by an audit company.

[6] As defined by the Accord, specialized lending consists of five categories: project finance, object finance, commodities finance, income-producing real estate finance and high-volatility commercial real estate finance. See items 218 - 228 of the Accord, for more precise definition of the types of specialized lending.

[7] Payment and settlement of bank's business activities are not included in this business line, but in the business line that includes the activity that caused such payment or settlement.

Once the division of activities in the eight business lines is over, the bank shall establish a system to ensure distribution of gross income into business lines. The bank shall take into account the gross income of each business line, to calculate the capital requirement for operational risk by applying the following formula:

$$K_{SA} = \frac{\sum_{1-3} \max(GI_{1-8} \times \beta_{1-8}, 0)}{3}$$, where:

K_{SA} - the capital charge under the standardized approach

GI_{1-8}- annual gross income in the given year for each business line

β_{1-8} - fixed percentage, set by the Basel Committee, relating the level of required capital to the level of the gross income for each business line:

Business lines	***β***
Corporate finance	18%
Trading and sales	18%
Retail banking	12%
Commercial banking	15%
Payment and settlement	18%
Agency services	15%
Asset management	12%
Retail brokerage	12%

Accordingly, the capital requirement is a three-year average of the capital requirement for operational risk arising from each business line. When the bank reports negative capital requirement for some business line, as a result of the negative gross income of such business line, it could finance such negative amount by the positive capital requirement (positive gross income) generated by other business lines in the same year. When the gross income of all business lines in one year is negative, such gross income shall not be taken into account in the calculation of numerator, but shall be included in the denominator that year. Therefore, regardless of whether the gross income is positive or negative, the sum of annual gross income shall always be divided by three.

This is the third difference between the basic indicator approach and the standardized approach when used for determining capital requirement. Besides the division of gross income by business line and the determined fixed percentages for each business line, these two approaches (basic indicator approach and standardized approach) differ in the way in which the negative gross income is used when determining capital requirement. In case of negative gross income of all business lines in any of the three last years, the amount of capital requirement determined by using the standardized approach would be lower. The reason behind such difference in the treatment of the negative gross income is the intention of the Basel Committee to encourage the banks to apply advanced approaches for calculating the capital

requirement for operational risk. In this case, as well, the national supervisor shall have the right (based on criteria defined in the second pillar of the Accord - supervisory assessment) to determine additional amount of capital requirement for a bank, if they consider that the resulting amount does not correspond with the bank's standing.

The fourth difference between the standardized approach and the basic indicator approach lies in the obligation for the bank to meet the exact criteria that make her eligible for using the standardized approach when determining capital requirement for operational risk. The Accord specifies basic criteria for the bank to become eligible to use the standardized approach, according to which the bank shall:

- make sure that the supervisory and management boards are involved in the monitoring of the operational risk management system,
- make sure that the operational risk management system is based on concrete elements and applies to the overall bank's operations,
- make sure that the bank holds ample resources to apply this approach and to establish proper control and audit.

These basic criteria should be supplemented by criteria related to principles the bank has to follow when dividing activities by business line. As mentioned above, the bank should have adequate policies in place to define criteria for division and distribution of gross income among business lines. These criteria should be regularly updated so as to include new business activities of the bank and changes thereto.

Besides the basic criteria, the Accord also defines additional criteria for application of this approach. They particularly refer to the method of establishment and use of the efficient operational risk management system in place, as follows:

- clearly defined rights and responsibilities of the bank's management bodies,
- monitoring of all data relevant to the operational risk management, particularly those concerning the considerable losses arising from exposure to this risk,
- establishment of a regular management information system on the bank's exposure to operational risk and on the losses, thus obtaining proper and timely data and information on operational risk exposure. The bank shall have procedures in place to help its bodies undertake informative measures,
- complete documentation of the operational risk management system,
- regular independent verification of the operational risk management system by the internal audit and audit company.

Banks that apply standardized approach may not decide to switch to the basic indicator approach, unless the national supervisor approves it. On the other hand, if the supervisor decides that the bank is no longer eligible for applying the standardized approach, it can require from the bank to cease using this approach, and to start calculating the capital requirement by using basic indicator approach.

3.2.1 Alternative standardized approach

In spite of the standardized approach, the Accord allows for application of so-called alternative standardized approach the bank may use, only if the national supervisor decides to allow this option. The national supervisor could decide to allow all banks to use this approach, or only banks that prove that the alternative standardized approach ensures more realistic calculation of the capital requirement for operational risk. The bank permitted to apply this approach can no longer use the standardized approach without approval of the national supervisor. The goal of the Basel Committee is to restrict the number of banks eligible for using this approach, and this approach is not recommended for large banks operating in developed financial markets.

The alternative approach also uses the gross income divided by business line as a basis for determining the capital requirement for operational risk, save for two business lines: retail banking and commercial banking. These two business lines use the average three-year amount of credits to and claims on those two sectors, times the corresponding fixed factor "m", rather than the gross income. The purpose is to avoid damaging of banks whose overall business is mostly constituted by these two business lines, making their gross income substantially larger compared to the gross income of other banks.

The amount of credits and claims is recognized on a gross basis, i.e. the amount of impairment is not taken into account. Credits to and claims on the business line of retail banking include credits approved to natural persons, small- and medium-size companies, retailers and claims purchased from these persons. Credits to and claims on the business line of commercial banking include credits approved to large corporations, government, banks and other legal entities regarded as corporations, specialized lending and claims purchased from those persons. Credits to and claims on the business line of commercial banking also include the carrying value of securities constituting the banking book.

The capital requirement for operational risk arising from retail banking and commercial banking shall be calculated by using the following formulas:

$$K_{RB} = \beta_{RB} \times m \times CC_{RB} \qquad K_{CB} = \beta_{CB} \times m \times CC_{CB}$$, where

K_{RB}, K_{CB} - capital requirement for operational risk arising from retail banking, i.e. commercial banking

B_{RB}, β_{CB} - Beta factor for retail banking, i.e. commercial banking (12%, i.e. 15%)

m - 0.035 (fixed factor)

CC_{CB}, CC_{CB} - credits to and claims on the business line of retail banking, i.e. the business line of commercial banking, as an average for the previous three years

The capital requirement for operational risk of these two business lines shall be added to the calculated capital requirement for operational risk arising from the other six business lines. The other six business lines shall use their gross income, and the fixed beta factors defined in the standard approach.

Besides the basic exception made in the alternative standardized approach in terms of using credits to and claims on business lines of retail banking and commercial banking, this approach also allows for the following three options:

- the retail banking and commercial banking to use the defined beta factors (12% and 15%, respectively), while all other business lines to use the same beta factor of 18%. This approach is particularly applicable to banks primarily involved in traditional banking activities,
- the retail banking and commercial banking to use one beta factor (15%), and all other business lines to use beta factors defined by the standardized approach,
- the retail banking and commercial banking to use one beta factor (15%), while all other business lines to use the same beta factor of 18%.

The national supervisor shall, under the Accord, identify criteria for a bank to become eligible for applying this approach. This means that the supervisor could require all or some of the criteria to be met for using the standardized approach.

3.3 Advanced measurement approach

With the introduction of advanced measurement approach, the Basel Committee allows the capital requirement for operational risk to be determined by using an internal model for operational risk measurement. The bank that applies this approach has to develop an internal model for determining the capital requirement, relying on its own experience and data available on the severity of losses by business line. This model aims to determine the bank's expected and unexpected losses arising from operational risk exposure. The sum of capital requirement for expected and unexpected losses provides the total capital, the bank has to allocate, for operational risk. The bank may allocate only capital requirement for unexpected losses, if it proves that the expected losses are properly covered otherwise (e.g. allocation of special reserve for risk events, adequate inclusion of the possibility for fraud or theft, in the bank's price for its products, etc.).

Expected losses are determined by using the average amount of losses for the bank at a specific past period. This type of losses includes losses produced by high frequency risk events, irrespective of the severity of losses, with high frequency/low severity losses being the most often. Unexpected losses include losses resulting from low frequency/high severity risk events.

The normal distribution function could be used for defining the level of expected and unexpected losses. Losses swinging around arithmetic mean (μ) with 99.9% confidence interval[8] are considered expected losses. Losses which, within the normal distribution, are beyond the defined confidence interval are unexpected losses for the bank as a result of operational risk exposure.

The national supervisor shall grant a license for application of the advanced measurement approach. To obtain such license, the bank should meet three types of criteria/standards: general, qualitative and quantitative as defined by the Accord.

[8] 99.9% confidence interval has been defined by the Accord.

The general criteria are identical with the basic criteria on the application of standardized approach. This approach will become eligible for regulatory purposes once the supervisor specifies a period of initial monitoring of its application. In this period the supervisor shall test the appropriateness and authenticity of the model to be applied by the bank.

The qualitative criteria are largely identical to the additional criteria to be met by the banks to become eligible for using the standardized approach. These qualitative criteria concern the method of organizing and operating the operational risk management system, and the Accord specifies precise must-have elements of the bank's operational risk management system.

The quantitative criteria for applying advanced measurement approach include establishment of a loss database, as a ground for determining expected and unexpected losses from operational risk exposure. The bank may establish this database by using various sources. The Accord defines the following basic sources of data: internal data, external data, scenario analyses and business environment and internal control systems of the bank. The bank shall define the extent to which each source could be used, so as to ensure objective calculation of the potential losses from operational risk exposure. The extent to which each source could be used should be transparent, documented and consistent.

3.3.1 Internal data

Bank's internal data on losses arising from operational risk exposure (risk events) are the best source of data for the development of an internal operational risk measurement model. Data on bank's losses are the most appropriate when they directly relate to its current business activities and processes. Hence, the bank should have documented procedures in place for assessment of the current relevance of historical data, including data on certain corrections (allowed exceptions, biased decision making). Bank's internal data could be used for calculating the capital requirement, if the bank meets the following standards defined in the Accord:

- if the bank has internal data on losses incurred in the period of at least five years. As an exception, banks that introduce advanced measurement approach for the first time are allowed to hold such internal data for a period of at least three years,
- if the bank divides available data by business line, as specified in the Accord[9]. The method of division and the criteria underlying such division has to be documented. This documentation helps the supervisor to verify and test the operational risk measurement model of the bank ,
- if the internal data include all material activities and operational risk exposures. The bank should seek to prove that all activities or exposures, on which internal data are not available, have no material effect on the overall risk level. For this purposes, depending on the work load and nature, the bank should determine the minimum amount of losses, the

[9] The same business lines used in the calculation of capital requirement for operational risk by applying standardized approach.

excess of which is considered material and included in the internal database (so called significant losses),
- if, apart from data on loss severity, the bank also collects data on the date of loss occurrence, the amount paid/collected later on, and descriptive information on the reasons behind, and the effect of, such loss.

Losses arising from risk events related to market risk exposure are part of the capital requirement for operational risk. Losses arising from risk events related to credit risk exposure (e.g. inappropriate collateral) are part of the capital requirement for credit risk.

3.3.2 External data

The bank should use external data, particularly on certain types of low frequency losses/risk events. These data could be used by the bank only if they contain information on the loss severity, nature and size of activity that lay behind such losses, the reasons and circumstances of loss occurrence, and other information useful for determining the risk event significance. The bank has to have a precisely defined process in place to identify cases that require use of external data, and to define methodology suitable for proper adjustment of such data to the needs and features of the internal model of the bank. The terms and method of using external data must be updated, documented and audited regularly.

3.3.3 Scenario analyses

Most frequently, scenario analyses are used to estimate the exposure to high severity risk events. Scenario analyses are developed by skilled and experienced operational risk management experts. They use their own experience to create potential risk events (scenarios) and to calculate the potential loss severity for each event. The purpose of scenario analyses is to calculate unexpected or catastrophic losses the bank could suffer as a result of low frequency/high severity risk events. These risk events could be discussed individually or as interrelated events, ensuring calculation of the total amount of loss for the bank based on several simultaneous risk events.

3.3.4 Business environment and internal control systems

Additionally, the bank's methodology for operational risk measurement has to take into account its business environment and the features of the internal control system. These factors could significantly affect the bank's operational risk profile, and should therefore be used as a source of data for calculating capital requirement. The bank should also determine the influence of changes in the business environment and the internal control system, on the overall risk profile and the loss severity. In this case, as well, all assumptions and factors must be confirmed through comparison with the amount of loss of the bank itself or with the external data available to the bank. If the comparison shows deviations, the bank will have to adjust its model to make it fit the current internal and external business environment of the bank.

3.3.5. Techniques for operational risk mitigation

The banks applying the advanced measurement approach can include adequately the effects of certain risk events insurance in their internal model, as well. The insurance recognition as a technique for operational risk mitigation is limited at 20% of the total amount of capital requirement determined with implementation of the advanced measurement approach. Also, such a reduction allowed by the Accord is possible only if the insurance fulfils the following conditions:

- The rate of the insurance company for payment of its liabilities is equal to or higher than „A";
- The minimum validity period of the insurance police should be one year. The bank is required to make adequate reductions to the insurance amount that is taken into consideration when determining the capital requirement for all policies with residual maturity shorter than 1 year. The insurance policies with residual maturity equal to or smaller than 90 days cannot be taken into consideration when determine the capital requirement for operational risk coverage;
- The cancellation notice of the insurance police should equal at least 90 days;
- The insurance policy should not contain any exceptions, or limitations in case of supervisory measures towards the bank, including also bankruptcy or liquidation;
- The calculation for operational risk mitigation should be transparent and it should mirror the banks' coverage with insurance;
- The insurance is provided by an entity that is not connected to the bank;
- The manner of insurance recognition is documented, while the bank publically announces the manner in which it uses the insurance as a technique for operational risk mitigation.

3.3.6. Problems in the implementation of the advanced measurement approach

The successfulness of the each internal model for determining of the capital requirement for operational risk coverage depends on the accuracy and the updating of the database on the basis of which it is developed. Hence, the largest problems that can arise from the application of the advanced measurement approach relate to the adequacy of the database for registered losses from different events. The most important problems are the following:

- The collection of the data on the registered losses from different events began recently, because of which both, their number and their type are limited;
- Having in mind the short period for data collection, the quality of those data is under question, especially those collected in the first several years;
- The internal data commonly fail to include the risk events that occur rarely, but usually cause huge losses (low frequency/high severity), because these events emerges only in few institutions. As a result, for such events the bank has to use external data or scenario analyses. In practice, the banks face with significant challenges for adequate combination of these different sources of data. The external data obtained from different sources can differ substantially, which depends on the size and the characteristics of the institutions these data originate from, as well as the system of internal control

of that institution. As a result, adequate adjustment of the external data on the bank's profile is required, for which quite bigger experience and knowledge is required;

- Having in mind the characteristics of the operational risk, problems about the precise distinction between losses originating from the exposure to credit or market risk and losses resulting from the exposure to operational risk occur. The differences between these three types of risks can be minor, because of which it is possible to include the same loss in the determining of the capital requirement for covering several risks. Although the Accord gives guidelines for resolving these problems, however, these double or triple effects are serious challenge in the practical development of the internal models of the banks;
- The Accord provides the banks with possibility to determine the minimal amount over which they will collect data on the registered losses (substantial losses) by their own. This amount can considerably differ from bank to bank, even with banks with similar characteristics and size. As a result, the possibility for using external data for covering those risk events for which the bank has not own base reduces;
- The databases usually fail to include losses that could emerge with the banks, but for some reasons they didn't occur (the so-called "near missess"). They are loses that did not happen, because of certain activities of third parties on which the bank did not have any influence, or because of certain activities in the bank itself which resulted in loss prevention (for example, timely police action for prevention of theft, or timely detection of embezzlement in the bank itself). In these instances, the bank fails to register losses, because of which those losses, in most of the cases, will not be part of its database;
- The banks that have established a system for rewarding of the employees on the basis of the attained results can face with cases when the employees do not report all losses, in order to attain adequate efficiency level. That, beside the need of good control systems for identification of these events, is to the detriment of the establishing of full database for the realized losses.

Having in mind the previous problems, as well as the high costs needed for development and maintenance of the internal model for operational risk measurement, the number of banks interested in the implementation of the advanced measurement approach is smaller. This approach is commonly used only by the banks being sure that its implementation will enable to determine more adequate amount of capital requirement for operational risk coverage, than the capital determined on the basis of other two approaches. Hence, only the large international banks with developed business networks are interested in the implementation of this advanced approach, which has already been approved in practice.

3.4. Partial implementation

The supervisor may allow the bank to implement the advanced measurement approach only for some of its activities, while for other operations it should use the other two approaches for determining capital requirement. Such a partial implementation is allowed in instances when the following conditions are met:

- All approaches provide coverage of the entire operational risk exposure;

- All activities covered with individual approaches meet the adequate criteria prescribed with the Accord;
- The advanced measurement approach covers the largest portion of the bank activities;
- The bank has plan for gradual implementation of the advanced measurement approach for all material activities. The plan should be prepared on the basis of real perceptions for the bank's possibility to move towards full implementation of the advanced monitoring approach.

2. OPERATIONAL RISK MANAGEMENT

The banks should establish operational risk management system, regardless of the approach they use in the determining of the capital requirement for operational risk coverage. The operational risk management means efficient identification, measurement, or assessment, monitoring and control, or mitigation of the operational risk. The adequate implementation of this process depends, to great extent, on how the bank bodies understand the importance and the characteristics of the operational risk and their capability for efficient surveillance of this process. All elements of the operational risk management should be stipulated in the banks' internal acts (policies, procedures). Also, having in mind the possible effects this risk can have on the bank, the successful operational risk management means also implementation of business continuity plan.

Each of these elements will be reviewed in details in this circular.

4.1. Role of the bank bodies in the operational risk management

The efficient management of the operational risk largely depends on the participation of individual supervisory bodies and the bank management, in order to establish and implement adequate policies, procedures and practices for managing this risk. The activities and the tasks of the individual bank bodies in the operational risk management are defined in the Banking Law and the Decision on the risk management prescribed by the National Bank. The general objectives that individual bank bodies should direct their activities to are given below.

The role of the Supervisory Board in the operational risk management should be focused on the establishing of the following:

- adequate environment in which every employee will be aware for the risk they are exposed to in the execution of their tasks (the so-called risk culture);
- general framework for operational risk management and clear guidelines for the other bodies and persons regarding the operational risk management;
- open cooperation and exchange of information on operational risk management and timely and accurate reporting on the operational risk;
- constant training of the employees, which will ensure uniform understanding and full application of the established operational risk management process in the entire bank.

The role of the Board of Directors and the Risk Management Board is to establish and implement general framework for operational risk management determined by the Supervisory Board. The banks should have efficient systems for reporting and monitoring of the operational risk, and where necessary, resolving of the problems arising from this risk. The efficiency of these systems can be ensured through the establishing of the so-called protection approach at three levels:

1. Protection at the level of business lines, i.e. at the level of the organizational units performing those business lines, including also the

units performing the ancillary activities of those business lines - the best results are achieved if each of the employees in these organizational units is informed and understands the types of risk events related to the tasks they perform, as well as on their role in the control and the operational risk mitigation;
2. Protection at the level of persons/bodies competent for operational risk management (person/organizational unit for risk management, person/unit for controlling the compliance of the bank operations with the regulations);
3. Protection through activities of the internal audit.

In order to ensure adequate environment and general framework for operational risk management, the adoption of written policies and procedures that will encompass all significant aspects of managing this risk is of considerable importance. The basic elements the policy for operational risk management should contain are prescribed in the Decision.

4.2. Operational risk identification

The process of operational risk identification should enable coverage of all risk events the bank is exposed to, regardless whether they are events that can, or cannot be easily quantified. Also, the established manner of identifying operational risk should enable encompassing also of all future risk events and factors. Hence, the efficient identification of operational risk should take into consideration the internal and external factors that could have negative influence on the bank's risk profile.

The internal factors are related to the nature of the activities the bank performs, its organizational structure and the changes in this structure, the quality and the change in the human resources etc. The exposure to the operational risk is bigger when the bank introduces new products or activities, wins new markets and/or performs business activities in the region, which are geographically distant from the bank's main office. Very frequently, the banks invest in the information technology as a technique for operational risk mitigation. However, such investment can have adverse effect. In practice, there are large number of examples when the use of automated processes causes transformation of the so-called small, but frequent losses into huge, but seldom losses.

One of the types of operational risk that can cause substantial losses for the bank is the use of outsourcing. On one hand, the transfer of part of the activities to the outsourcing provider and the use of their experience and knowledge in the respective area, can reduce the banks' risk profile. On the other hand, the use of outsourcing does not lessen the responsibility of the bank bodies for the manner certain activity is performed in. The bank bodies remain to be responsible for ensuring safe and efficient operating of the outsourcing provider and adherence to the respective legal framework. Oppositely, the inappropriateness of the outsourcing provider and the services it provides can have negative influence on the bank operations.

These factors related to the bank operations should be accompanied with the external factors, as well, such as the changes in the bank operations and the technological development. These factors have adequate influence also on the level

of operational risk the bank is exposed to and which should be taken into consideration in the management of that risk.

It is especially important to apply the approach to the operational risk identification in all organizational units in the same manner, i.e. each organizational unit of the bank should understand equally each type of risk event which represents exposure to operational risk.

4.3. Assessment or measurement of the operational risk

Beside the identification of the operational risk, the bank should estimate also the vulnerability to this risk, which will enable better understanding of the own risk profile and better distribution of the necessary resources for operational risk management.

According to the international practice and experience, there are several instruments for assessing the operational risk, as follows:

- **Self assessment of the risk** - the bank assesses the own operating and activities it performs in order to determine the potential risk events. This process is carried out with the bank itself (internally) and it can include filling-in of various questionnaires/lists regarding the operational risk (checklists) and/or organization of workshops in the bank for the exposure to operational risk. The self assessment can include the following elements: description of how the operational risk is understood, identification of different events, determining of the bearers (persons, organizational units, products, or services, systems, etc.) of those events, determining the persons that should undertake adequate activities for control and mitigation of the operational risk, etc.
- The banks can use **matrixes (scorecards)** which convert the qualitative assessments into quantitative volumes that enable ranking of different events. These matrixes can be used by banks for determining capital requirement for covering operational risk, which arise from each business line;
- **Risk grouping** - individual organizational units, functions or processes are grouped by the type of the operational risk. The risk grouping can enable determining of the individual risk events, their mutual correlation, as well as the area where there are weaknesses in the operational risk control. This manner ensures to set the priorities in the activities to be undertaken for the purpose of adequate operational risk management;
- **Risk indicators** - They are mostly financial indicators that depict the banks' risk profile. These indicators should be revised on a regular basis (monthly, or quarterly) for the purpose of timely identification of the changes which can have negative influence on the risk level. Examples for such indicators can be the following: number of failed trading, rate of change in the human resources, frequency and/or the error and omission extent, etc.;
- **Scenario analyses** – as mentioned before, it is an instrument that is commonly used for determining unexpected losses with rare events, but which can cause extremely huge losses. For adequate implementation of the scenario analyses, it is extremely important to accurately determine

their elements, such as the defining of the scenario, the source and the type of the data which are used, the frequency of these analyses, the manner of determining of the influence of the losses on the profitability and the solvency of the banks, etc.

The so-far experience in the implementation of these instruments for assessment of the operational risk shows that the banks mostly use own assessments of risk. Thus in 2004, the credit rating agency "Fitch rating" conducted an analyses on the 50 largest banks of Australia, Canada, Europe, Japan, South Africa and USA[10]. Out of the total number of analyzed banks, 65% selected their assessments as a manner for measuring operational risk. This analysis also shows that in future, the banks expect mounting significance of the risk indicators.

4.4. Monitoring and reporting on the operational risk

The regular monitoring of the operational risk enables timely identification of the problems or the deficiencies in the policies, procedures, or practices for managing this risk. It is a basis for undertaking timely measures for eliminating the determined problems/deficiencies, which from its part, contribute to the reduction of the number and the volume of the realized losses.

For efficient monitoring of the operational risk, the bank can set **thresholds of the risk indicators** which it uses to measure this risk, or to establish **early warning system**. These indicators should take into consideration the potential sources of operational risk, such as the fast development, the introduction of new products, changes in the human resources, errors in the execution of transactions, or in the functioning of the information systems, etc.

On the basis of the utilization of some of the previous assessment instruments and on the basis of the data on the bank's previous experience with the losses due to certain bank activities, the bank can also establish **database on losses** arising from risk events. These databases represent quantification of the losses occurring as a result of the exposure to operational risk. In order to use these data efficiently, the bank should establish a system for monitoring and recording of the necessary data. However, only the data the bank manages with, based on its experience (internal data), may be used, as well as the data obtained from external sources, thus widening the database for operational risk management.

The databases should encompass all realized losses, as well as the losses from events that did not happen for certain reasons ("near missess"). The database can include information on the following: the type and the date of the risk event, the loss amount, the bearer of that event or the weaknesses in the control systems, the amount of the possible return on assets (for example, as a result of use of techniques for operational risk mitigation), the undertaken activities and the drawn moral for the weaknesses in the operational risk management system. These databases can refer to all losses regardless of their amount, or only to those losses

[10] Source: Operational Risk Management & Basel II Implementation: Surveys Results – FitchRatings, April 2004.

that the bank finds considerable (determining minimal loss amount over which the bank enters data in the base[11]).

Such a manner of loss quantification and use of adequate database is a ground for development of internal models for operational risk measurement. These models integrate the quantitative sources of data and the qualified information. The trend of development of own models for operational risk measurement is especially evident in the few previous years, which was adequately influenced also by the advanced approach of operational risk measurement within the Basel Capital Accord.

4.1.1. Reporting system

The bank should ensure adequate system for reporting to the adequate persons or bodies in the bank. The reporting of the operational risk should be timely and regular, in conformity with the nature and the amount of the operational risk the bank is exposed to in its operating.

The reports for the operational risk exposure can contain different data that depicts the areas (business lines, organizational units, transactions, operations, or other events), facing with operational risk. From this aspect, the reports for the operational risk can refer to the following:

1) individual risk events which realized operational risk loss in the previous period, stating also the main reasons for the loss, the loss amount and the untaken measures. This type of reports can arise from the loss database, if any in the bank;
2) the level of operational risk in the banks, which includes also identification of those areas registering increase in its level. This type of reports most commonly contains the data/results obtained from using the instruments for assessment or measurement of the operational risk and the data on the amount of the risk indicators, or the early warning system indicators.

Regardless of the manner of preparation of the operational risk reports, the reporting should cover all identified problems and to represent a basis for undertaking timely and efficient additional measures for operational risk coverage/mitigation.

The reports are submitted to the adequate bank bodies, in accordance with the bank's organizational structure and depending on the competencies of each body. Besides undertaking of adequate measures, the reports should also be used for improving the current operational risk management system, as well as development and improvement of the current policies, procedures and practices.

4.5. Control and mitigation of the operational risk

For the purpose of establishing control at the level of operational risk, the bank should make analysis which will enable to determine the following:

[11] This minimum amount can refer to all events that are exposure to operational risk, or the bank can determine the minimum amount for each event.

- the risks it will accept as part of its operating, and which will cover by allocating respective level of capital, or through their inclusion in the prices of the products/services it offers;
- the risks that will be taken and that will be subject to control, or mitigation, including their transfer to third persons through risk events insurance;
- the risks it will not accept (avoid risks).

As for the risks to be taken by the bank, the Supervisory Board and the Board of Directors should create conditions where the control activities will be an integral part of the bank's regular activities. In this manner, timely and fast response to the changes in the external and internal factors will be ensured, as well as reduction or avoidance of redundant costs.

As aforementioned, one of the basic manners for ensuring adequate control of the operational risk is to establish risk culture and clear rules for ethical behavior of the employees. The banks having such rules in place are more prepared to deal with all risk events more efficiently and there is smaller possibility for registering loss as a result of those events.

The efficient control system means adequate distribution of responsibilities, especially from the aspect of the avoidance of conflict of interests. The inadequate segregation of duties can cause the persons or the bodies registering conflict of interests to cover the losses, errors, or the inadequate activities undertaken, or made, by their part. Hence, the potential cases for conflict of interest should be identified, reduced to minimum and regularly monitored and analyzed.

Beside the adequate segregation of duties, the efficient control system should include also the following:

- constant monitoring of the adherence to the established threshold of the risk indicators;
- defining of the possibility for access and use of the bank's assets and its data;
- employment of high quality and professional personnel with high ethical standards;
- identification of the business lines, or the products where the yield amount fails to meet the real expectations (for example, the low risk and margin trading ensures high yield, which can mean that the yield is a result of non-adherence to the internal control limits);
- establishing remuneration policy which is in line with the bank's long-term strategy;
- regular training of the employees about the operational risk, the most significant risk events, the manner of control and mitigation, etc.;
- rules for using vacation leave which will prescribe mandatory absence from work within longer period (for example, using vacation in the period no less than two consecutive business weeks);
- regular verification and settlement of transactions and accounts.

The failure to establish and apply such control practices is most frequently a reason for registering larger operational losses with the banks.

Beside the internal control system, the operational risk can also be mitigated by using reduction techniques. Namely, the probability that certain types of risk events will occur is minor, although their occurrence most frequently has huge negative influence on the bank's financial standing. Those types of risk events, for example, the natural disasters, cannot be controlled. As a result, the bank should have adequate techniques, or programs for reducing the exposure to operational risk, i.e. for its transfer to third parties. The most common example of techniques for reducing the exposure to operational risk is the conclusion of insurance policies for certain risks the bank accepted to take. The bank bodies (usually the Supervisory Board) should determine the rules for using the insurance as instrument for operational risk mitigation. It means defining of the risk events this instrument will apply to and the terms under which it will be used.

It should be taken into consideration that the instruments for operational risk mitigation through its transfer to third parties cannot be considered as adequate replacement for efficient control system, but only as a supplement to that system. Also, the bank should conduct regular analysis on the benefit and the costs for using the insurance policies, analysis of the real level of operational risk transfer[12] as well as the analysis of the probability for emergence of other risk types[13].

4.6. Business continuity plan and contingency plan

Because of the reasons that are beyond bank's control, certain risk events can prevent the bank to continue to perform part or all activities. Such events are most frequently related to the damages, or problems with the telecommunication or information infrastructure. The terminations can cause substantial losses to the bank, as well as more serious destructions in the financial system functioning. Because of these reasons, it is especially important for the banks to establish and manage business continuity plan, which will include several possible scenarios for potential danger from termination of the bank operations. Therefore, the bank is required to identify those business processes which are critical for its operating, including also those that are related to the outsourcing. For these processes, the bank should identify the alternative manners for business continuation. Special attention should be paid to the possibility for data recovery (electronically or in hard copy), which are crucial for business continuity. If these data are maintained on reserve location, or in case when the operating should carry on other location, the bank should ensure these locations to be on adequate distance from its primary location (for example, from its main office), in order to mitigate the risk from simultaneous damage of data on both locations.

An integral part of the business continuity is the plan for operations in extraordinary conditions. This plan separately defines the technical and the organizational measures and activities for reestablishing, i.e. continuation of the operations and minimization of the consequences from the business termination, i.e. from deterioration of the working conditions.

[12] The level of operational risk still present with the bank (which is not transferred to third party).

[13] For example: occurrence of counterparty risk or country risk as a result of transfer of the risk to third party coming from other country.

The banks should revise the business plan continuity regularly in order to ensure harmonization with the current activities, business processes and strategies. Also, this plan should be tested periodically in order to check its applicability, as well as to determine the bank's readiness for its efficient implementation[14].

[14] Having in mind the significance of the business continuity plan and the contingency plan of the bank, their contents and scope are defined in details in the Decision.

3. OUTSOURCING

When using outsourcing, the bank should take into consideration the influence each deviation from the quality or continuity in the services provided by these entities may have on its regular operating, the possibility for efficient risk management and the internal control system, as well as on its clients. The decision clearly emphasizes the banks' obligation about managing risks which can occur in these instances. More detailed overview of all aspects the bank should take into consideration in the operational risk management, which can arise from the utilization of outsourcing, such as: defining of the outsourcing services that can expose the bank to operational risk, establishing and implementation of the policy for using outsourcing services, and assessment of the outsourcing risk, selection of outsourcing provider, defining of the contents of the agreement and continuous oversight of the services the outsourcing provider provides.

5.1. Defining of outsourcing

Outsourcing means use of services that can expose bank to operational risk. They are services the bank could perform by itself and which enable the bank to perform the financial activities, including also the services that serve as support to the execution of those activities. In that regard, the bank cannot transfer the implementation of the financial activities, but only the services, which support their implementation. The bank cannot transfer to third parties neither the activities of the bodies which, pursuant to the Banking Law are prescribed as mandatory (internal audit, risk management, adherence to the regulations).

On the other hand, the standardized services, such as use of the services of the interbank communication systems and interbank communication and trade the use of telecommunication network and infrastructure, the marketing services, the maintenance and cleaning services and other utility services, services for market research, procurement of goods and construction material, lease of real estate etc. are not considered as outsourcing.

In practice, there are many instances when one contract concluded with third party covers a lot of services, only small part of which can expose the bank to operational risk. In these instances, the bank should have clear picture for segregation of different services, from the aspect of the exposure to operational risk and on that basis, to include in the agreement adequate provisions, according to the requirements of the Decision and the guidelines provided in this circular.

5.2. Outsourcing policy

Pursuant to the Decision, if, when performing the financial activities the bank uses outsourcing, it is required to have outsourcing policy in place, which contains at least the elements prescribed in the Decision. The main objective of the policy is to cover, through its provisions, the entire process: adoption of decision on providing outsourcing, their selection, conclusion of the contract, assessment and monitoring of the risks related to the use of outsourcing, the manner of oversight of the operations of the outsourcing provider from the aspect of the services it provides to

the bank, as well as reporting to the bank bodies on the exposure to outsourcing risk.

For the purpose of adequate implementation of the policy, the bank should define the role and the responsibility of the persons/organizational units competent for selection of the outsourcing provider, the conclusion of contracts and monitoring of the operations of the outsourcing provider. Regardless of the use of outsourcing as a support to the financial activities the bank performs, the implementation of those activities remains within the responsibilities of bank bodies, which are required to provide all conditions for performing of the activity pursuant to the regulations and the internal acts of the bank.

5.3. Assessment of the outsourcing risk

For the purpose of adequate risk management, the bank should primarily make adequate assessment of the risk level and the possibility for control of that risk. For that purpose, the bank should assess the following factors:

- influence of the use of outsourcing on the profitability, reputation, or business continuity;
- the potential losses the bank clients can register, if the outsourcing provider fails to fulfill adequately its commitments regarding the services it performs;
- the capability of the outsourcing provider to perform the services in conformity with the strategic and business needs of the bank;
- the influence of the use of outsourcing on meeting the internal or prudential indicators and adherence to the legal regulations;
- the total amount of costs for using outsourcing;
- the influence of the connection of the outsourcing provider with other entities on the bank operations;
- regulatory treatment of the outsourcing (whether it is subjected to supervision);
- importance and the complexity of the processes/services which will be transferred to the outsourcing provider;
- possibility for risk control when the bank uses several outsourcing providers;
- possibility for performing activities by the bank, if the outsourcing provider fails to perform its liabilities pursuant to the concluded contract.

5.4. Selection of outsourcing

The selection of the outsourcing provider should be based on adequate analysis of its operating. For that purpose, the banks should develop own criteria for selection of outsourcing provider on the basis of which it can assesses the capability and capacity of the outsourcing for timely, quality and efficient response to the bank needs. Among the criteria the bank should undertake are also the following:

- experience of the outsourcing provider for the adequacy of its capacities for implementation of the specific service;
- reputation and market share of the outsourcing provider;

- financial standing of the outsourcing provider (for example through analysis of the last revised financial statements);
- suitability of other entities the outsourcing provider uses for performing the specific service;
- the experience of other persons in the use of outsourcing;
- capability of the outsourcing for efficient reaction in case of temporary prevention from providing services, regardless of the reason for that deterrence.

The bank shall pay special attention when using outsourcing from foreign entity. In that instance, the foreign entity is more restricted to react on time, which should be taken into consideration when selecting. In that regard, the bank should estimate also the economic, legal and political standing of the domicile country of the outsourcing provider. When selecting the foreign outsourcing provider, the bank should determine whether the regulations of the domicile country of the outsourcing provider fails to restrict the National Bank in its right to perform oversight over the operating of those entities, or the agreements concluded with those entities, pursuant to the Banking Law.

5.5. Defining of the contents of the contract with the outsourcing provider

The use of outsourcing must be determined with conclusion of written contract which will clearly determine the rights and responsibilities between the bank and the outsourcing provider. The written agreement is important mean for risk mitigation in case of improper execution of the requirements by the outsourcing. As a result, the contract should be written clearly and precisely in order to ensure full completion of the commitments. With the contract, the bank should define at least the following elements[15]:

- clause for possibility from early termination of the agreed obligations upon bank request;
- provisions for protection of the secrecy of the bank's data;
- provisions for ensuring harmonization of the outsourcing provider with the adequate regulations;
- provisions which enable the bank smooth access and possibility for control of the premises and the data of the outsourcing, regarding the services it performs on the behalf of the bank.

The banks should ensure easy access and possibility for control of the premises and data of the outsourcing provider for both the National Bank and the audit company which performs audit on the annual financial statements of the bank. That access should refer exclusively to the data and information with the outsourcing that refer to the services that bank performs for the bank[16].

[15] These elements are also defined in the Decision.

[16] For example: if the bank engages person/entity for collection of its claims, the right of access refers to the data and information which pertain to the claims that the outsourcing provider charges on the banks' benefit, and not to all other data and information of the outsourcing.

Despite the minimal elements prescribed in the Decision, the bank can include in the contract also the following provisions that enable to determine the rights and responsibilities of both counterparts: description of the activities that are subject to the contract, requests regarding the quality of the services, responsibility in case of damage or violation of the agreed responsibilities, obligation for the outsourcing company to request prior written consent from the bank in case of engagement of subcontractors, defining of the manner in which the bank will perform oversight over the operations of the outsourcing, enabling adequate conditions for performing immediate oversight of the outsourcing provider by the National Bank, pursuant to the Banking Law[17], type and the contents of the reports the bank will obtain, or it can request from the outsourcing provider, as well as other provisions envisaged in the regulations for regulating the contracting relations.

5.6. Bank's oversight of the outsourcing

After the selection of the outsourcing provider and conclusion of the contract, the bank is required to monitor its operating and implementation of the concluded contract constantly. For that purpose, the bank should primarily have adequate professional staff which can monitor the operations of the outsourcing provider and which will manage with the business relations with that person in adequate manner.

The constant oversight should refer at least at the following: monitoring and analysis of the quality of the activities the outsourcing provider performs on the behalf of the bank, monitoring of all factors that can cause need for modification of the concluded contract, analysis of the financial standing of the outsourcing provider, as well as monitoring of the possible changes in the human resources, the management, ownership, or organizational structure of the outsourcing, which can have adequate influence on the efficient and quality execution of its contractual obligations to the bank.

Skopje, July 21, 2011

Manager
Natasa Andreeva

[17] Pursuant to Article 128 of the Banking Law, the National Bank may conduct inspection of the operations of the entities providing ancillary services to the bank. In instances when the outsourcing, as defined in the Banking Law, is deemed as company for providing ancillary services to a bank, the National Bank may conduct inspection of the operations of that entity.

REFERENCE

- Banking Law ("Official Gazette of the Republic of Macedonia" no. 63/2007, 90/2009 and 67/2010)

- Decision on the risk management ("Official Gazette of the Republic of Macedonia" no. 14/2011)

- Decision on amending the Decision on the methodology for determining capital adequacy ("Official Gazette of the Republic of Macedonia" no. 31/2009)

- International Convergence of Capital Measurement and Capital Standards – A Revised Framework Comprehensive Version – Basel Committee on Banking Supervision, June 2006

- Sound Practices for the Management and Supervision of Operational Risk - Basel Committee on Banking Supervision, February 2003

- Outsourcing in Financial Services - Basel Committee on Banking Supervision, February 2005

- Guidelines on Outsourcing – Committee of European Banking Supervisors, April 2009

- Smjernice za adekvatno upravljanje rizikom eksternalizacije – Hrvatska Narodna Banka, Listopad 2005

- Operational Risk Management & Basel II Implementation: Surveys Results – FitchRatings, April 2004

- The Oldest Tale but the Newest Story: Operational Risk and the Evolution of its Measurement under Basel II - FitchRatings, January 2004

- Moody's Analytical Framework for Operational Risk Management of Banks – Moody's Investors Services, January 2003

- Enhancing frameworks in the standardized approach to operational risk – Financial Services Authority UK, October 2010

- Sound Practices for the Management and Supervision of Operational Risk (Consultative Document) - Basel Committee on Banking Supervision, December 2010