OPERATIONAL-RISK MANAGEMENT IN A BANK

Wincenty KULPA and Antoni MAGDOŃ
Bank PeKaO, S.A. Rzeszow, Poland, wkulpa@vp.pl

I. Introduction

Risk is present in every aspect of human life, but in the context of conducting all kinds of activities, and especially business activities, it deserves special attention. And through effective risk management it is possible to achieve the effective functioning of business entities. This issue gains a special meaning in the context of banks which are public-trust institutions, whose goal is to maximise their market value.

Numerous crisis phenomena we have witnessed over the last few years, whose consequences had to be to different degrees faced by banks, started with operational problems. That is why banks and their managerial staff, especially since the economic crisis that started in 2007 with the collapse of the subprime-loans market in the USA, have been putting special stress on effective operational-risk management. The crisis has imposed more demanding requirements in this area, as very often the maturity of operational-risk management systems influences not only the results of a bank's activities, but also its survival.[i] Research carried out in 1997 by the British Bankers Association and Coopers & Lybrand has shown that for almost 70% of the surveyed banks operational risk is equal to or even more important than market risk or credit risk.

The original research on operational risk focussed on its negative definition, according to which operational risk was understood as the so-called residual risk that included aspects outside market or credit risks.[ii]. With the development of the banking-services sector the definition of operational risk also evolved, and defining it correctly became an important element that could ensure successful operational-risk management.[iii]

The key moment in the evolution of operational-risk definition was the publishing by the Basel Committee of a document on operational-risk management in banks.[iv] The fact that the Basel Committee on Banking Supervision raised this issue proved that risk management had become an issue that was too important to dismiss in a "new capital agreement". It contains a full, final and clear definition of operational risk which is defined as *"the risk of loss resulting from inadequate or*

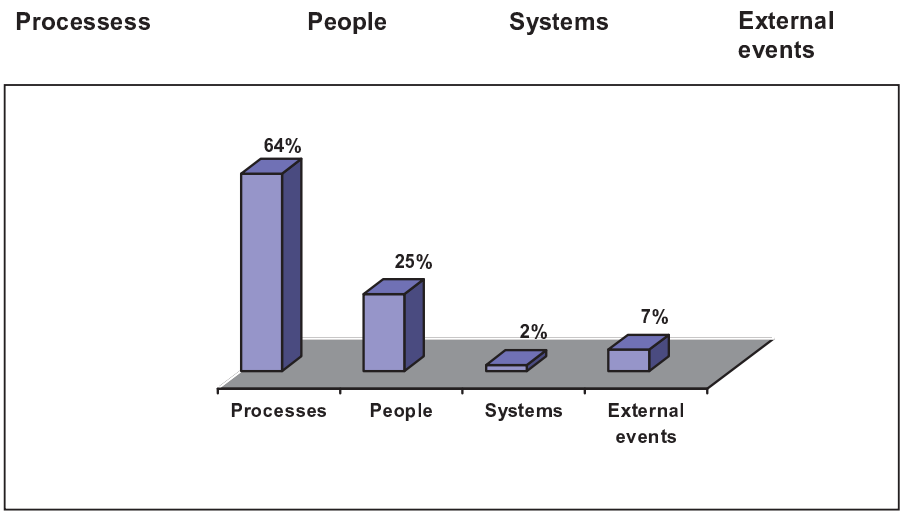
failed internal processes, people or systems or from external events", and this definition also included legal risk[v].

Based on the operational-risk definition formulated by the Basel Committee it needs to be noted that it stresses the following operational-risk factors:

- processes,
- people,
- systems,
- external events.

On the basis of the research conducted by the Risk Management Association, different levels of participation of individual factors in operational risk were determined, as presented in the figure below.

Fig. 1. The influence of individual factors on operational risk.



Source: Risk Management Association webpage - www.rmahq.org.

Apart from the definition by the Basel Committee on Banking Supervision, many other operational-risk definitions exist in relevant literature, e.g. P. F. Maryland defines operational risk as *"the risk of loss connected to failure when handling a transaction for the client"*, R. Kendall defines it as *"the risk connected with a loss as a result of defective systems operations, insufficient control,*

improper management or human error", M. Iwonicz-Drozdowska and A. Nowak defined operational risk as: *"the risk resulting from errors during settling accounts or performing transactions that are made by the bank's staff or technical appliances",* R. Kałużny writes that *"operational risk is the result of internal and external factors caused by the inefficiency of systems, unintentional or intentional failures in human actions and also natural disasters and catastrophes",* L. Sołtysik sees the institution in the face of danger as the source of operational risk.[vi] One of the definitions that is closest to the initial definitions of operational risk is presented by R. Jemeson, who determines it as *"any source of threat not considered to be a credit or market risk*"[vii].

It is important to mention here the research carried out in 1999 by three institutions: the British Bankers Association, the International Swaps and Derivatives Association and the Risk Management Association, in which banks were asked to give an operational risk definition, and the research carried out in 2003 by "Operational Risk" Magazine [viii], that indicated that each of the banks defines operational risk in an individual way. However after the results of this research were compiled, four basic definitions of operational risk emerged:

- Operational risk is the risk of fraud committed by employees or persons outside an organisation, and the risk of conducting unauthorised transactions or errors caused by IT systems.
- Operational risk is the risk that results from systems maladjustment, operational problems, breaching guidelines developed by internal auditors, fraud, and unpredicted catastrophes causing unpredicted losses for the organisation.
- Operational risk should be viewed from the point of view of the effectiveness and integrity of the systems of control and other mechanisms whose aim is the implementation of business processes.
- Operational risk is endangering the company with financial and non-financial losses caused by unpredicted events or failures in operational-systems processes. [ix]

II. Operational-risk factors

Irrespective of the adopted definition, operational risk occurs in every financial unit, and the financial condition and public trust of such an entity, especially of a bank, depend on its proper management.

In order to properly manage operational risk in a bank it is vital to get acquainted with its main reasons. The operational risk factors that are mentioned by banks most often are:

- people – that is, the broadly-understood quality of resources, skills, motivation, the ability to use appliances and equipment correctly and the conditions of work,
- safety connected to human resources and also to banks' client-service systems (personal data protection, bank information access channels),
- processes and systems – i.e. the integrity of the business, IT and technical processes,
- products – that is the method of new-products implementation, the preparation of the portfolio in respect of business, law and IT,
- links between clients, - i.e., relations between clients and the bank in respect of the field of economy and ethics,
- outsourcing, - i.e. external contracting of processes and services,
- crimes,
- failures, catastrophes, disasters.

Many of the factors enumerated by the banks are reflected in the relevant literature on operational risk. Special attention should be given to J. Bessie, who enumerates the following as the primary operational-risk factors:

- people,
- processes,
- applied models of risk measurement and assessment,
- IT systems.[x]

D.N. Chorfas, on the other hand, does not focus on factors that cause operational risk, but on its elements, where he distinguishes:

- the risk of improper supervision,
- the risk of improper management
- the risk of the lack of professionalism,
- the transaction risk
- the risk connected to payments,
- the risk connected to concluded agreements,
- the risk connected to the bank's operational back office,
- technological risk.[xi]

III. The classification of operational-risk

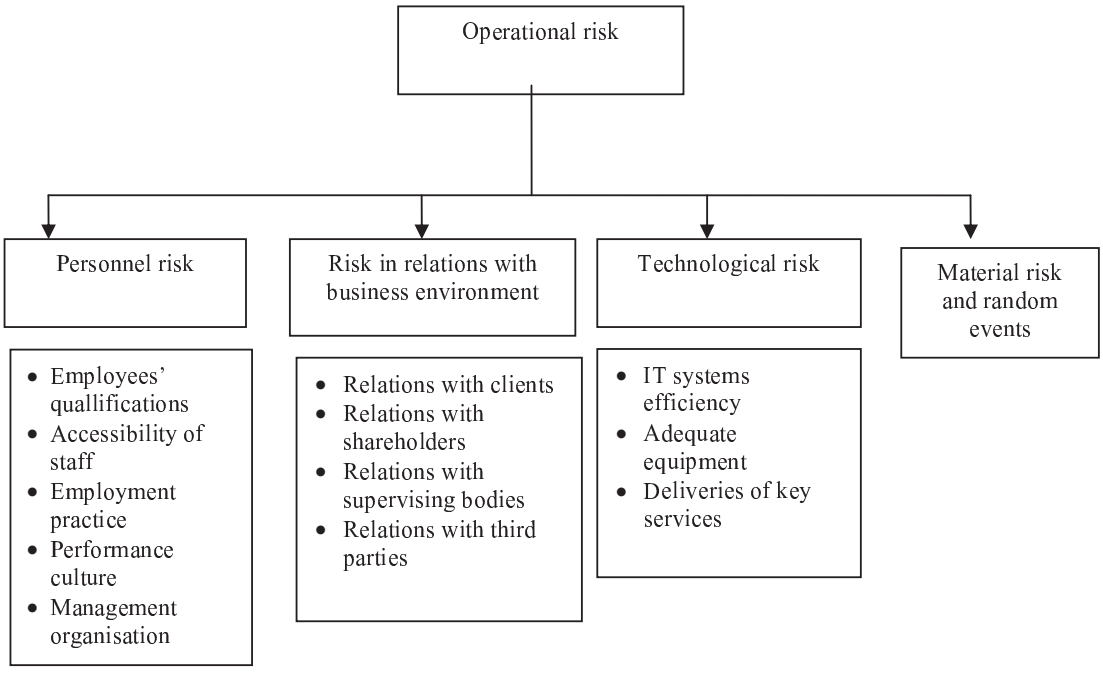
Taking into account the main causes and elements that are included in operational risk, it may be divided into:

- the risk that is personal in character, connected to staff qualifications, intended or unintended actions to the detriment of the bank, performance culture, staff responsibility, and management organisation.

- The risk that is organisational in character, resulting from, e.g. an inappropriate organisational structure, internal audit rules, accounting, and planning.
- The risk that is material or technical in character, connected with technical appliances owned by the bank and financial-operation abilities necessary for the bank's functioning.
- The risk of relations with the business environment, resulting from relations with shareholders, clients, supervising authorities and third parties.
- Material and random risk[xii]

The division of operational risk is not closed. With the developing economy, the changing social and technological reality has considerable influence on both operational-risk definition and its types. That is why most of the banks are elaborating on their own operational-risk management policy, just like they are elaborating on their credit policies. In a document relating to operational-risk management policy there are basic areas of banking activities where individual types of operational risk are identified.

Fig. 2. The classification of operational risk



Source: J. Krasodomska, "Zarządzanie ryzykiem operacyjnym w bankach" (Operational-Risk Management in Banks), PWE, Warsaw 2008, p. 19.

IV. Operational-risk measurement

In an operational-risk management system its measurement is an important, if not the most important, issue. It is extremely difficult, however, as it concerns many areas of a bank's activities. Nevertheless, it is indispensable, as it:

- is a condition for creating methods of operational-risk management
- is a tool indispensable for managing the risk connected with particular transactions,
- allows the reduction of operational costs incurred by the bank,
- encourages managers to design and use the methods of operational-risk management which give a chance to gain higher profits.[xiii]

According to the publications by the Basel Committee, a bank can apply three different approaches to measuring operational risk:

- A simplified approach: based on the capital requirement resulting from operational risk, calculated on the basis of one particular total-risk exposure indicator, that is, the average net income for the last three years. The capital charge in this case constitutes 15% of this value, i.e. the capital requirement = 0.15 x average gross income.[xiv]
- The standard method: in order for a bank to introduce this, it has to have an operational-risk management system that meets the Basel Committee's minimal requirements for use by a bank. With this method, banks identify and define the amount of profit from eight lines of business. The size of the reserve for each of the lines is calculated by multiplying gross profit by a constant indicator defined in the range 12% to 18%. The capital requirement of operational risk is the sum of encumbrances resulting from lines of business. The definitions of the lines of business and the respective factors are presented in Table 1 below. The total capital requirement of operational risk is the three-year arithmetical average of the required encumbrances estimated separately for each year. The negative values, in the case of a gross loss in the line of business, may be used to reduce positive encumbrances from the lines of business.[xv]
- Advanced Measurement Approaches (AMA): applied by the banks that meet higher risk-management standards. In this method the banks themselves assess their exposure to operational risk and adjust the value of the operational-risk capital encumbrance, and, in the case of the purchasing of operational risk insurance, capital requirements are reduced by a

maximum of 20%. The application of this procedure is related to the obligation of having an A-rating by an external insurer, concluding an insurance agreement for a period of at least a year, a clear definition of the operational risk range, and the lack of exclusions and restrictions resulting from legal regulations. [xvi]

Table 1. Operational risk – the standard approach – the level of factors in relation to lines of business.

Lines of business	Factor (%)
Financial counselling	18
Trading in securities	18
Retail banking	12
Corporate banking	15
Payments and settlements	18
Agency services	15
Assets management	12
Brokerage	12

Source: Heffernan, "Nowoczesna Bankowość (Modern Banking), PWN, Warsaw 2007, p. 240.

Out of the three basic approaches, two basic methods of operational risk measurement have been designed in practice: the statistical method and the method based on the analysis of future events scenario.

The statistical method includes the disaggregation of operational risk onto the risk connected to systemic failure, frauds committed by bank employees and clients, the destruction of internal documentation etc. It can further distinguish individual classes of risk (it mainly concerns the banks performing numerous transactions and having, respectively, extensive databases). After performing disaggregation of risk, or its subdivision into individual classes, the respective probability of the occurrence of unfavourable events that could influence the bank is assigned. In this method losses incurred by the bank are presented as the frequency of such an event.

The method based on the analysis of future events scenario consists of defining the development of the future bank conditions in the context of the bank's financial results and of defining the frequency of future losses. This method is used when a statistical method cannot be applied.[xvii]

V Areas and stages of operational-risk management

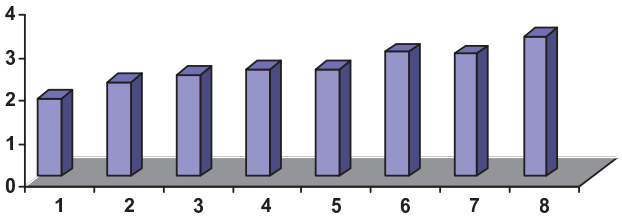
The Basel Committee, after it had held consultations with banks, distinguished basic areas where operational risk is usually present, and these include:

1. Real capital – the risk is connected to fixed-asset failures, disruptions to activities, systemic problems and difficulties in debt recovery and transfer of cash. In this area, technical failures, especially of IT systems play a leading role. Most of the banks have classified data-coding systems, updated in real time, created in case of the failure of the main system. A quick return to the market by the banks whose headquarters were destroyed in the September 11 attacks is a perfect example of efficient operational-risk management related to a given area. It was possible thanks to back-up copies of the accounting computer systems.
2. Human capital - the risk connected with human errors, problems in the area of employment procedures, work safety and embezzlement. The examples of the activities that influenced this area of operational risk may be as follows: mistakes when entering the amounts of purchase/sales orders, fines on a bank for breaching health-and-safety regulations, etc.
3. The law – the risk connected with possible lawsuits against the bank and connected with, e.g. improper client service, defects in the marketed products, and improper business practices. Numerous banks were sued by disappointed corporate clients who accused the banks of improper counselling in the field of its activities or financial investments. The most costly example for banks of improper handling of a client was in the year 2003, when investment banks located in New York unofficially admitted to taking advantage of the conflict of interest between investment banking and risk analysis departments (as part of a settlement with the Attorney General of New York State, the banks were not obliged to admit to committing offences but they had to pay considerable fines and cover the costs of the settlement). [xviii]
4. Fraud – the risk that may have external and internal sources is connected with both the banks' employees and the hacking circles and with elites and financial institutions. The case of Robert Maxwell's misappropriation of employees' pension funds, which affected banks for whom those funds constituted securities, may be an example in this area.[xix]

When analysing the areas influenced by operational risk we should pay attention to the elements that impact the implementation of the operational-risk management systems, which is shown in Figure 2, and elements that delay the implementation of the operational-risk management systems in Figure 3. The most

important factors that influence the implementation of the operational-risk management system are legal frameworks and internal regulations of banks that constitute the framework and the basis of formulating an effective operational-risk management programme.

Fig. 3 The elements that influence the implementation of operational-risk management systems.



1. **Offers of a new capital agreement (Basel) and domestic legislation.**
2. **Developing new internal procedural models.**
3. **Concerns about internal operational losses.**
4. **Others (e.g. development of an infrastructure counteracting money laundering).**
5. **Individual (joint) initiatives in respect of operational risk.**
6. **The pressure from shareholders on operational-risk management and disclosing information on losses.**
7. **Accounting scandals and the regulator's reaction.**
8. **Terrorist attacks (the issue of maintaining business continuity).**

NOTE: 1 – the most important, 4- the least important.

Source: E. Leander, An exclusive survey shows a reality gap, "Operational Risk", June 2003, vol. 4, No. 6, p. 28.

The factors that delay and have a negative influence on the implementation of effective operational-risk management systems result from difficulties in homogenous and clear operational risk specification. They are the result of the three basic stages in operational-risk management, that include:

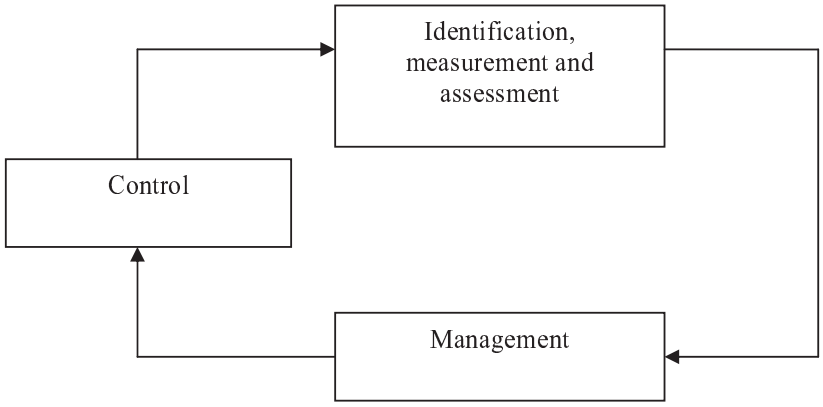
- Risk identification, measurement and assessment,
- the control of undertaken activities,
- risk management.

The first stage, i.e. risk identification, measurement and assessment belongs to management's scope of obligations. On the basis of the available information, it should identify the operational-risk types present in the given bank and measure it, with the use of an applicable method. Then the management performs total risk assessment and they undertake activities connected with it.

Stage two, i.e. the control of undertaken activities, is connected with both the control of the presence and implementation of activities connected to operational risk, and also the control of the functioning of instruments that are used to reduce the risk. Constant monitoring and the flow of information on the activities connected to operational risk and the effectiveness of instruments reducing the negative effects of the presence of a given type of risk facilitate the proper functioning of the third stage of risk control, that is, risk management.

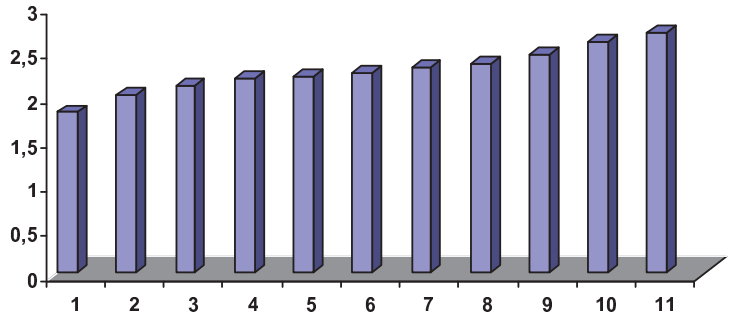
The third stage uses and combines all the information obtained in the first two stages of operational-risk management. Through the proper implementation of activities that reduce the risk and the knowledge on their efficiency, we may, in a reduced way, manage the risk and its size.

Fig. 4. The stages of risk management.



Source: Own study on the basis of J. Krasodomska, „Zarządzanie ryzykiem operacyjnym w bankach" (Operational Risk Management in Banks), PWE, Warsaw 2008, p.34

Fig. 5. The elements that delay the implementation of operating-risk management systems



1. **Difficulties connected with operational risk modelling.**
2. **Difficulties connected with the application of historical data.**
3. **Difficulties connected with the mixing of qualitative and quantitative information.**
4. **Difficulties with ensuring proper quality data.**
5. **The cost and time of implementation**
6. **No clear instructions on the part of the regulators.**
7. **Difficulties with data assessment/reporting.**
8. **Organisational-structure fear of introducing changes**
9. **Systems integration issues.**
10. **Access of qualified staff.**
11. **Insufficient engagement of the management in the project.**

NOTE: 1 – the most important, 4- the least important.

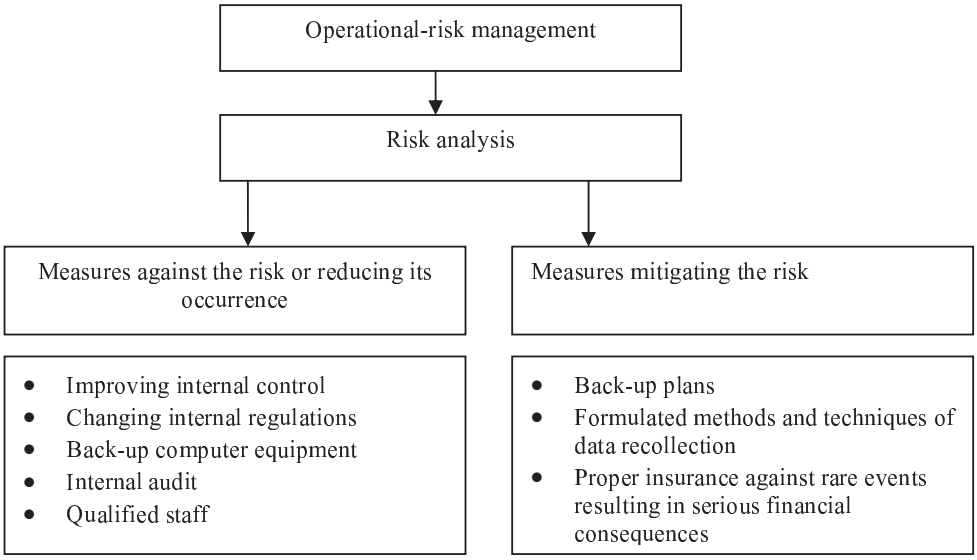
Source: E. Leander, An exclusive survey shows a reality gap, "Operational Risk", June 2003, vol. 4, No. 6, p. 29.

In the situation where the occurrence of operational risk and potential loss is very low, a passive strategy may be assumed, that is the passive observation of risk. In the remaining situations it is necessary to undertake activities that include the elimination of the causes of risk, as presented in the Figure below [xx].

When observing the new areas of a bank's activities [21, 22, 23], it is possible to distinguish a number of activities and tools used in the operating-risk management process. The basic ones are as follows:

- selecting people with proper qualifications,
- organisations and coherent risk-management systems,
- introducing internal regulations and instructions and the implementation of procedures,
- skills in the assignment of decisions
- Properly-managed accounting, records, and data processing registration systems,
- Managing information that is properly correlated with a system for entering data, reporting, monitoring and periodic auditing,
- internal control and supervision.

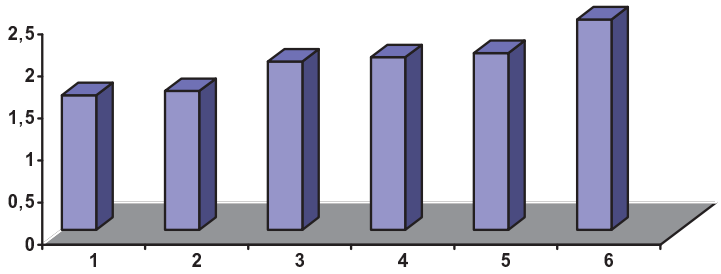
Fig. 3. Operational-risk management



Source: J. Krasodomska, „Zarządzanie ryzykiem operacyjnym w bankach", (Operational-Risk Management in Banks), PWE, Warsaw 2008, p.36.

The correct combination and implementation of these activities and tools should result in the effective management of the operational risk, which in turn will produce financial and image-related benefits for banks (Fig. 6). However, only constant monitoring, control and continuous assessment of the level of risk can minimize its impact on the bank's financial results [24].

Fig. 7. The benefits arising from the implementation of the operational risk-management system



1. **Reduction of operating losses.**
2. **Improvement in management and financial results obtained.**
3. **Protection against damage to goodwill.**
4. **Improved reporting.**
5. **Optimisation of the economic capital.**
6. **Other.**

NOTE: 1 - the most relevant, 4 – the least relevant.

Source: E. Leander, An exclusive survey shows a reality gap, "Operational Risk", June 2003, vol. 4, No. 6, p. 28.

VI. Summary

The increasingly-frequent and spectacular bankruptcies and financial problems of global companies have made operational-risk management an important topic. The examples of ineffective management of the operational risk include:

- The Barings Bank – a loss of USD 1.3 billion for the bank, which went bankrupt in February 1995, after the dealer Nick Leeson assumed a prominent position, far exceeding the bank's equity, on the derivatives and options markets, which generated losses following the earthquake in Kobe, Japan. A detailed analysis of this case showed that the failure was not

basically caused by financial risk, but rather by the operational risk related to poor internal control and external audit, the insufficient knowledge and experience of the senior staff in respect of derivatives, and too complex an organizational structure.

- The Allied British Bank – a loss of USD 691 million, after the dealer, Jon Rusnak, did not arbitrate between option prices, forward prices, and spot quotations to diversify the risk, but carried on forward transactions. This was possible due to the insufficient control of the derivatives units, too much trust in the employees and the poor internal and external controls.

The above examples prove that bank risk cannot be efficiently managed without taking operational risk into account. This risk, encompassing numerous aspects of bank activities, is connected with their development, the availability of new financial instruments and the world's civilization and economic progress. To let banks develop and tailor to the clients' needs, the reasons, effects and methods of operational-risk management have to be examined. As much as the operational risk stemming from random events and relations with business circles can only be limited through proper management, the operational risk connected with HR and technologies can be almost entirely liquidated through optimum control, surveillance, and a security and training system.

Despite the operational risk being constantly analysed, it will continue to evolve along with the development of banking and financial instruments. That is why banks will have to thoroughly understand, constantly monitor and control this risk in order to guarantee fail-safe protection against it.

References:

[i] D. Benyon, *Leeds Must , "*OpRisk&Compliance", June 2009.
[ii] P. Jorin "Value at Risk", McGraw-Hill, New York 2001, p. 451
[iii] M. Power "The invention of operational risk", the ESRC Centre for Analysis of Risk and Regulation, CARR Discussion Paper Series, London 2003
[iv] The Basel Committee on Banking Supervision "Operational-risk management", Bank for International Settlements, Risk-Management Group, Basel 1988
[v] The Basel Committee on Banking Supervision "The International Convergence of Capital Measurement and Capital Standards - a Revised Framework" Bank for International Settlements, Basel 2004, pp.137-8
[vi] J. Krasodomska,"Zarządzanie ryzykiem operacyjnym w bankach" (Operational-Risk Management in Banks), PWE, Warsaw 2008, pp.16-18
[vii] N. da Costa Lewis, "Operational Risk with excel and VBA, Jon Wiley and Sons", New Jersey 2004, p.2.
[viii] The Corporate Governance Survey 2003, Part 1, On Risk Disclosure; a Long Road Ahead, "Optional Risk 2003, vol.4, no 6.
[ix] The British Bankers Association, The International Swaps and Derivatives Association and the Risk-Management Association,"Operational Risk, The Next Frontier, The British Bankers Association, London 1999.
[10] Emilia Vasile, Human Resource planning, chapter 3 from book "Human Resources management. Concept and Practice", LAP Lambert Academic Publishing, 2012, pp. 17-23
[11] J. Bessis, "Risk Management in Banking", Wiley and Sons", London 2003, pp. 20-21.
[12] D.N. Chorafas, "Reliable Financial Reporting and Internal Control. A Global Implementation Guide, Jon Wiley & Sons, New York 2000, p. 191.
[13] Jaworski W.L, Zawadzka Z."Bankowość zagadnienia podstawowe" (Basic Banking Problems), Poltex, Warsaw 2005, pp. 309-310.
[14] R. Kałużny,"Pomiar ryzyka kredytowego banku" (Bank's Credit Risk Measurement), PWN, Warsaw 2009, p.32.
[15] P. Heffernan,"Nowoczesna Bankowość" (Modern Banking), PWN, Warsaw 2007, p.241.
[16] The Basel Committee on Banking Supervision, The International Convergence of Capital Measurement and Capital Standards: A Revised framework, Basel 2004, pp. 139-140.

[17] The Basel Committee on Banking Supervision, The International Convergence of Capital Measurement and Capital Standards: A Revised framework, Basel 2004, pp. 140-141.
[18] R. Kałużny,"Pomiar ryzyka kredytowego banku", PWN, Warsaw 2009, p.32.
[19] P. Heffernan,"Nowoczesna Bankowość", PWN, Warsaw 2007, p.135.
[20] P. Heffernan,"Nowoczesna Bankowość", PWN, Warsaw 2007, p.135.
[21] J.Krasodomska,"Zarządzanie ryzykiem operacyjnym w bankach", PWE, Warsaw 2008, pp.16-18.
[22] R. Štefko, P. Dorčák, F. Pollák „Shopping on the internet from the point of view of customers", Polish Journal of Management Studies 2011 vol.4, p. 220
[23] A. Targowski, V. Modrak "Is Advanced Automation Consistent with Sustainable
Economic Growth in Developed World?", Proceedings of Enterprise Information Systems International Conference Part I, , Vilamoura, Portugal , Springer , 2011, pp 63-72.
[24] I.C. Dima, S. Vladutescu „Persuasion Elements Used in Logistical Negotiation: Persuasive Logistical Negotiation" LAP Lambert Academic Publishing, p. 368.
[25] P. Matkowski "Zarządzanie ryzykiem operacyjnym"(Operational-Risk Management) Wolters Kluwer, Kraków 2006, p. 52.
[26] Emilia Vasile, Ion Croitoru "Integrated Risk Management System – Key Factor of the Management System of the Organization", chapter 12 in the book „Risk Management", InTech, Croatia, 2012, pp. 253-284