New tendencies of management and control of operational risk in financial institutions

Pjotrs Dorogovs\textsuperscript{a}, Irina Solovjova\textsuperscript{b}, Andrejs Romanovs\textsuperscript{c}, a\textsuperscript{*}

\textsuperscript{a}\textsuperscript{*}Riga Technical University, Riga, 1658, Latvia
\textsuperscript{b}University of Latvia, Riga, 1586, Latvia

Abstract

Nowadays, financial institutions highly recognize a great influence of effective risk management on profit abilities. Therefore risk management became an important part of the financial instrument. According to the latest researches, there still remain problems related to the management of various types of risks. For instance, the Basel Committee of the Bank of International Settlements imposes financial institutions for more intensive devoting their attention to operational risk management problems. Due to the increased intensity of performed financial operations, financial institutions became very vulnerable to operational risks. In many cases, the high level of operational risks is conditioned by IT system failures.

Keywords: Stability, banking system, operational risks, information technology

1. Introduction

The stability of the banking plays an important role in the long-term economy growth. The weakening of the banking system of any country represents a threat for the financial stability both in the particular country as well as abroad. In the modern world the role of banks exceeds the framework of money and credit relations. The modern bank represents a supermarket of financial services. It is impossible to imagine normal, rational organization of economic activity without banks. Namely this is the reason why the institutions of banking supervision are now facing the task to promote the strengthening of the financial health of the banking system. Namely because of this all parties should be interested in the successful management by banks today and in the ability to meet future challenges. The responsibility for this, first of all lies with banks themselves, however, also the banking supervision institutions must play an important role in providing banks with the possibility of balanced management and reasonable capitalization.

\textsuperscript{*}Corresponding author. Tel. +371-26338312 fax. +371-67089513

Email address: pjotrs.dorogovs@rtu.lv

© 2013 The Authors. Published by Elsevier Ltd.
Selection and peer-review under responsibility of the International Strategic Management Conference.
The banking crises, which have occurred both in transition economies and developing countries in the last 10 years, have strengthened conviction about the importance of a stable and well regulated banking system. Therefore, an increasing amount of attention has been paid to ensuring its stability and analyzing its development.

The stability of the banking system can be defined as the ability of it to function in a sustainable equilibrium under different economic circumstances and ensure that the system does not require infusions of external resources to maintain its operations. The history of development of banking systems shows that regulation and management are required to achieve this state quantitatively and qualitatively.

The necessity of strengthening the financial system is becoming the problem that attracts increasing attention all over the world. The ways for strengthening financial stability on the global scale has recently been searched by the Basel Committee of Banking Supervision and International Settlement Bank as well as International Monetary Fund.

The main global trend in the development of bank supervision is increasing of its efficiency. By increasing of efficiency we mean better execution of its main tasks without proportional increasing of the resources allocated for this purpose. The trend can be described as increasing of the productivity of the banking sector. It is supported by the following changes in the system of the bank supervision:

- Improvement of the organizational structure of the institutions of bank supervision. Here we have to point out the transition from the principles of universalism and functional homogeneity to the principles of functional and productive specialization of substructures as well as development of the subordinary links in the structure;
- Improvement of the interaction between the internal and external bank audit that represents an important instrument in the provision of the stability of banks.
- Improvement of the supervision instruments. The basic components of this direction are:
  1. improvement of the technique of analysis and evaluations (use of the process modeling – stress testing, i.e., assessment of the stability of the system under certain unfavorable operation conditions) as well as transition from assessing the level of certain risks to complex assessment of the quality of the risk management);
  2. creation of organizational conditions that provide for effective adoption of optimal decisions.
  3. increasing of the staff qualification.
- Transition from the extensive model of supervision to intensive. It is expressed in the specification of the supervision object. Intensive supervision model is based on the methodologies aimed at establishing the areas of increased risk in the operation of the credit institutions and concentration of supervision resources in these areas.

The approach has been given the name of the risk-based supervision.

There is no general agreement on the most suitable definition of risk for economists, financial specialists, decision theorists, and insurance theorists (Moosa, 2007). As a result, in different areas, different types of risks and, respectively, different risk management methods are considered. In business, four main general types of risk can be recognized: strategic, market, credit and operational risks (Jordan, 2005; King, 2001; Walker, 2001; ITG, 2007). The conducted research analyzes topical issues of operational risk management, connected with informational technology application.

2. Literature Review And Hypotheses

2.1. Risk Management Strategies of Commercial Banks and their Relationship to Economic Fundamentals

A modern concept of strategy has been defined in the XX century by J. Von Neumann and O. Morgenstern [3]. According to these authors, a strategy is a set of actions by the firm, which is determined by a particular situation. Later the concept of strategy has been made more precise, for example, by defining it as a model of plans, policies, tasks, objectives and opportunities designed to reach previously specified goals (Learnned, 1969).

The first literature devoted to the stability of the commercial bank system and management of stability has appeared only in the second half of the XX century — and its appearance was related to the end of the Bretton Woods system. Economic research in the second half of the XX century has considered the problems of achieving and sustaining a stable economic equilibrium. Theoretical aspects of the stability of banking system have been reflected in academic research by G. Schinasi (Schinasi, 2004), J. Sinkey (Sinkey, 2002), as well as work done by the International Monetary Fund (Houben, 2004) and the European Central Bank (ECB, 2004).

A particularly topical question is which factors influence the stability of the banking system. The first empirical research, which analyzed the relationships between the conditions of financial sector and economic growth have shown that there is a relationship between economic and financial development (Goldsmith, 1969; McKinnon, 1973). The question of causality between the level of economic and financial development, however, remains open. Boyd and
Honohan, for example, considered the impact of inflation on financial market and financial sector performance (Boyd, 2000; Honohan, 2003).

2.2. Requirements to operational risk management

Within this paper the following operational risks management documents are reviewed: The New Capital Accord Basel II, The Sarbanes-Oxley Act, Latvian FCMC Recommendations for Operational Risk Management.

The purpose of the International Convergence of Capital Measurement and Capital Standards (New Capital Accord Basel II) is to increase the reliability and stability of the international banking system (Basel, 2004). For this purpose the modern risks management technologies should be implemented. New Capital Accord Basel II claims to cardinaly modernize bank information systems. New Capital Accord Basel II requirements, which may correspond to the operational IT risk management, can be listed as follows (ITG, 2007):

- IT risk management: board of directors should be aware of the need for an operational risk management framework; develop policies, processes and procedures for managing operational risk; identify and assess the operational risk; regularly monitor operational risk profiles and material exposures to losses; have policies, processes and procedures to control and or mitigate material operational risks; have a framework in place to identify, assess, monitor and control mitigate material operational risks;
- IT internal audit: operational risk management framework is subject to effective and comprehensive internal audit;
- IT ensure continuous service: to have contingency and business continuity plans;
- IT escalation to management: sufficient public disclosure.

Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act) highlights the fact that the effectiveness of internal control system is directly dependent on the effectiveness of IT control activities system (ITG, 2006). An external monetary and financial institutions audit covers their financial departments, IT infrastructure, internal IT processes, as well as the IT departments’ personnel. In general, Sarbanes-Oxley Act defines several
requirements to ensure the IT governance that must be reached by the monetary and financial institutions top-level management [Sarbanes-Oxley, 2002]:

- regular reviews of exactness and completeness of financial reports (sec. 302);
- regular reviews of effectiveness of internal control evaluation and reporting system, including external audit (sec. 404);
- regular reporting about any significant facts and risks that may influence financial indicators (sec. 409).

It should be noted that the section 404 has the most influence on IT governance; this section emphasizes continual improvement procedures within corporate information system, based on the effectiveness of internal control system. In accordance with this section, top-management shall:

- state the responsibility of management for establishing and maintaining an adequate internal control system;
- contain an assessment of the effectiveness of the internal control.

Like the aforementioned documents, operational risk management recommendations developed by the Financial and Capital Market Commission of the Republic of Latvia, do not define certain IT requirements. Still, these recommendations indicate the necessity for operational risks management system and regular operational risks assessment, which can be obtained through the effective system of IT management and control. Thus, the requirements, which may correspond to operational IT risk management, are (LRFCMC, 2006):

- to implement management of such operational risks, which are associated with unauthorized external access to information resources and improper operating with customers confidential information (paragraph 4);
- to realize institution top-management responsibility in operational risks control system development and to control the efficiency of operational risks management techniques (paragraph 9, paragraph 10);
- to ensure operational risks regular identification and assessment (paragraph 12, paragraph 13);
- to realize continuity of institutions activities, which also include information technology and telecommunication infrastructure (paragraph 25).

This paper proposes two hypotheses:

**H1**: Operational risk management increases the stability of financial institutions.

**H2**: Internal information stealing and misusing became one of most important factors affecting operational risk management and control in financial institutions.

### 3. Methodology

#### 3.1. Research Goal

The goal of the conducted research is to identify and analyze topical issues of operational risk management in financial institutions, connected with informational technology application.

#### 3.2. Sources of operational risks

Systematization of sources of operational risks that affect the information and technology assets is crucial since implementation of which may have an impact on the confidentiality, availability and integrity of these assets. All sources of risks can be divided into four main classes: 1) human actions, 2) software and hardware failures, 3) weaknesses of internal processes and 4) external events. Each class is divided into subclasses and individual elements.

| Human actions | Software and hardware failures | Weaknesses on internal processes | External events |
|---------------|--------------------------------|---------------------------------|-----------------|
| Unintentional actions: | Equipment failures: | Design and implementation process: | Disasters: |
| - bug | - lack of capacity | - inadequate process | - weather conditions |
| - ignorance | - lack of productivity | - improper process | - fire |
| - noncompliance | - improper maintenance | - improper documentation of the process | - flood |
| | - obsolescence of equipment | - lack of understanding of | - earthquake |
| | | | - riot |
Internal offences remain one of the most topical issues for risk managers in the business sector. Economical fluctuations may generate great fraud or misuse desires – as soon as employees come under financial pressure they may face temptation of information stealing or misusing it for conducting auspicious trade deals of this information thus ensuring good profits for themselves on one hand and jeopardizing IT security on the whole and business data security in particular on the other.

As long as national economic remains flaccid with high level of unemployment Information security scams will remain serious problem. Also it's useful to remember that usually it takes 2-3 years to uncover already conducted fraud that means that misuses which took place in midst of crisis in 2008-2009 will be revealed only now.

Rapid and steady grow of internal information stealing and misusing has been tracked in previous five years. In the end of 2012 it grew by 52%. Also it should be noted that starting with late 2011 camerred employees started to cooperate in order to overcome modern data-theft protection systems making few smaller data transfers instead of one big, making usage of mentioned systems almost useless.

Also available applications for data theft now can be obtained over the Internet. Recently such applications became available as kits making them easier to use even for unprofessional. Furthermore data storage devices such as phones, USB sticks, players etc. are now used everyday by almost everybody, making them ideal environment for new types of infections and information loss.

Typical attacks using standard hardware and software features are:
- malicious code such as viruses and worms;
- unauthorized access to the company's business critical data;
- unauthorized change and transfer of this data to other people.

Three network protection levels for solution of banking systems network security can be distinguished:
- physical protection level. At this level physical access banking systems infrastructure and other network hardware is controlled;
- intra-company level. At this level staff access to certain information is regulated;
- an external level. At this level corporate information resources and technologies that can be accessed be external network user, for example, the customer, are determined.

| Deliberate actions: | Software failures: | Process control: | Legal problems: |
|---------------------|--------------------|-----------------|----------------|
| misuse              | incompatibility    | lack of monitoring| inadequacy     |
| fraud               | improper configuration management | lack of metrics | changes in legislation |
| sabotage            | improper management of change | lack of periodic review | litigation |
| theft               | incorrect security settings | improper possession process | |
| vandalism           | insecure programming practices | | |
|                     | improper testing   | | |

Service dependencies:
- supply problems
- dependence on emergency services
- transport problems
Fig. 2 Classification of Threads

Table 2 Enterprise Approach to Risk Management

| Internal Controls     | Misuse Management Controls | System and Data control                   |
|-----------------------|----------------------------|------------------------------------------|
| Internal Policies     | Prevention                 | Policy Based Framework                   |
| Education             | Detection                  | Vulnerability management and Compliance  |
| Hiring Practices      | Recovery                   | Strong Access Management                 |
| Secure Authentication | Forensics                  |                                          |
| Models                |                            |                                          |

Intrusion (in this case Misuse) detection is a method to effectively protect the bank IT system from possible attacks. As a supplement to firewalls, Misuse detection systems can provide additional options for systems dealing with possible frauds, expand the ability of system administrator to assure information security, and promote the completeness of information security in three main information security aspects.

Profiling the end user behavior is the most important aspect of data protection while focusing on Operational risks. Besides that software and network activities is not less important aspect since this method is effective in detecting external attacks that constitute almost two-thirds of the corporate system security. In information systems based on UNIX or Linux operating system, the sequences of shell commands are easily collectable and analyzable information, thus being the source material for creating profiles of end users, in addition to collecting of such information does not use significant system resources. On the other hand taking into account the difference between the behavior of end users, building profiles of their activities is a difficult task comparing to building a profile of program behavior. Hackers can even try adapting their behavior to fool IDS systems.

In recent years majority of research activities in the area of Misuse and Fraud detection is focused on studying the behavior of end-users and the creation of their profiles based on system call log files. Until now simple Misuse detection method based on monitoring system calls initiated by the active and privileged processes of used system is widely used. Profile of end-user normal behavior is constructed by enumerating all unique system calls, which are observed in log data being considered as daily normal, in turn, previously undetermined sequences are considered abnormal. This approach has been extended by various other methods. It was suggested to utilize data mining approach
to study samples of the system calls and construct small set of rules contained in normal data. During the monitoring and detection, the sequences that violate these rules are treated as anomalies and misuses.

4. Conclusions

As it was previously mentioned in the paper internal information stealing and misusing grew by 52% in the end of 2012. Obviously taking this fact in to account author can accept hypothesis of this paper – internal information stealing and misusing has become one of most important factors affecting operational risk management and control in financial institutions. Currently great part of risk management activities, in particular in all types of financial institutions, are focused exactly on preventing and combating internal fraud incidents and cases.

Also it should be noted that successful risk management (all types of risks should be taken into account as IT risks as various operational risks) would drastically optimize institutions’ running costs therefore increasing as overall Key Profit Indicators as also the stability of financial institutions. Above mentioned is leading to a conclusion that also first hypothesis of the paper can be accepted.

During preparation of this paper analysis of existent literature devoted to the stability of the commercial bank system and management of stability was conducted. Results showed that such literature became available only in second half of past century. Significant part of accessible paper works are dated by early 2000 and later.

Also topical issues of operational risk management in financial institutions were identified and analyzed. Systematization of sources of operational risks that affect the information and technology assets was performed and sources possible sources of such risks were divided in four classes: 1) human actions, 2) software and hardware failures, 3) weaknesses of internal processes and 4) external events.

Furthermore Misuse detection systems were analyzed. The results showed that currently available systems may help utilize the so called “End-user behavior profiling” method especially in information systems based on UNIX or Linux operating system where sequences of shell commands are easily collectable and analyzable information, thus being the source material for creating profiles of end users thus as a supplement to firewalls, Misuse detection systems can provide additional options for systems dealing with possible frauds, expand the ability of operational risk management teams to assure information security, and promote the completeness of information security in three main information security aspects.

References

Basel Committee for Banking Supervision (2004), International Convergence of Capital Measurement and Capital Standards: A Revised Framework, Basel Committee for Banking Supervision.
Boyd H., Smith D. (2000), The Impact of Inflation on Financial Market Performance, Journal of Monetary Economics.
Dorogovs P., Romanovs A. (2012), Modeling and evaluation of IDS capabilities for prevention of possible information security breaches in a Web-based application. Int. Conf. on Harbor Maritime and Multimodal Logistics,HMS 2012, Wien, Austria,pp.165-170.
European Central Bank (2004), Financial Stability Review, December 2004, ECB
Goldsmith R.M. (1969), Financial Structure and Development, New Haven.
Honohan P. (2003), The accidental tax: Inflation and the financial sector, Unpublished manuscript, The World Bank.
Houben A., Kakes J. and Schinasi G. (2004), Towards a Framework for Safeguarding Financial Stability, Department of International Capital Market, 2004 June, IMF.
IT Governance Institute (2007), IT Control Objectives for Basel II. The Importance of Governance and Risk Management for Compliance, IT Governance Institute.
IT Governance Institute (2006), IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control over Financial Reporting. IT Governance Institute.
Jordan E., Silcock L. (2005), Beating IT Risks, John Wiley & Sons.
King J. (2001), Operational Risk: Measuring and Modelling, John Wiley & Sons.
Learned E., Christensen Andrews R.C., Guth W.D. (1969), Business Policy: Tests and Cases, R.D. Irwin.
LRFCMC (2006), Recommendations for Operational Risk Governance. Latvian Republic Financial and Capital Market Commission (in Latvian).
McKinnon, R. (1973), Money and Capital in Economic Development, Brookings.
Moosa I. (2007), Operational Risk Management, Antony Rowe, Chippenham and Eastbourne.
Romanovs A., Merkuryev Y., Kilmov R., Solovjova I. (2008), A Technique for Operational IT Risk Management in Latvian Monetary and Financial Institutions, 8th WSEAS International Conference on Applied Computer Science, Venice, Italy, pp 230-235.
Sarbanes-Oxley (2002), Public Company Accounting Reform and Investor Protection Act, US Federal Law.
Schinasi G. I. (2004), Defining Financial Stability, IMF Working papers 2004 October, IMF.
Sinkey Joseph F. Jr. (2002), Commercial Bank financial managements in the Financial-Service Industry, Upper Saddle River, New Jersey, USA.
Teilans A., Romanovs A., Merkuryev Y., Kleins A., Dorogov P., Krasts O. (2011), Functional Modelling of IT Risk Assessment Support System, Economics and Management, No16, pp.1061-1067.

Walker S. (2001), Operational Risk Management: Controlling opportunities and threats, Connley Walker Pty.