ISSN 1407-7493 COMPUTER SCIENCE DATORZINĀTNE 2008-7493

INFORMATION TECHNOLOGY AND MANAGEMENT SCIENCE
INFORMĀCIJAS TEHNOLOĢIJA UN VADĪBAS ZINĀTNE

THE DEVELOPMENT OF THE OPERATIONAL IT RISKS MANAGEMENT CONCEPT

Ruslan Klimov, Mg.sc.ing., Ph.D. student, Department of Modelling and Simulation, Faculty of Computer Science and Information Technology, Riga Technical University, 1 Kalku Street, Riga, Latvia, e-mail:ruslans@itl.rtu.lv

Albert Reznik, Member of the Board, Baltic International Bank, 43 Kaleju Street, Riga, Latvia, e-mail:albert.reznik@bib.lv

Irina Solovjova, Dr.oec., Lecturer, Institute of Finances, Faculty of Economics and Management, University of Latvia, 5 Aspazijas Blvd., Riga, Latvia, e-mail:irina.solovjova@lu.lv

Jans Slihte, Dr.sc.ing., Director, IT Department, Ministry of Finance of the Republic of Latvia, 1 Smilsu Street, Riga, Latvia, e-mail:jans.slihte@fm.gov.lv.

Keywords: operational risks, risk management, IT governance

1. Introduction

Nowadays, monetary and financial institutions highly recognize a great influence of effective risk management on profit abilities. Therefore risk management techniques 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 [5]. It should also be admitted that the management of operational risks is close connected to information technology application.

Consequently, appropriate information technology is the foundation and facilitator of the operational risk management framework [7]. On the other hand, information technology can be pointed as a vulnerable area, which can be affected by additional external and internal risks with dire financial consequences. Accordingly, common IT management requirements indicate the need for careful IT risk management with the purpose to decrease the level of operational risks. The goal of this paper is to develop operational IT risk management concept that could be implemented within Latvian monetary and financial institutions.

2. Operational IT risk management in Latvian monetary and financial institutions

There is no general agreement on the most suitable definition of risk for economists, financial specialists, decision theorists, and insurance theorists [3]. 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 [1, 2, 4, 7].

2.1. Operational risks definition

An operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events [5]. Operational risks relate to all phases of the business process, from original through to execution and delivery, covering the front, middle and back office. These risks cover all areas linked to potential failures in the overall operation of a financial services organization and, specifically, the underlying technology and infrastructures [7]. Traditionally it is assumed that most operational risks arise from human internal or external activities. Internal human activity failures can be caused by an employer, an employee or a customer. These threats might be the risk of incorrect transaction during data input process, the risk of insufficient information system management or internal information theft. The external human risks can be characterized by outside attacks. The process risk causing factors are connected to events resulted from a firm's execution of business operations. System factors correspond to the loss events resulting from a disruption of service or from technology failures. Finally, external events are loss events caused by natural and unnatural events that threaten the ability of the firm to continue operations.

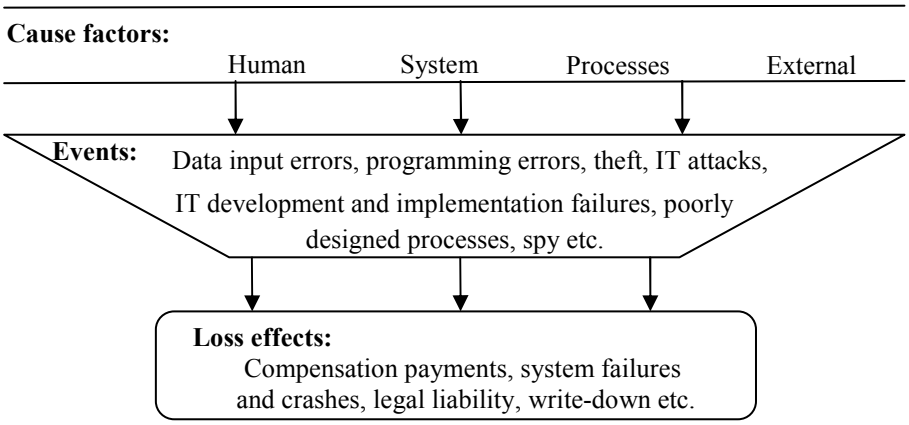

Figure 1. Examples of causes, events and effects of operational risk

The above reasoning gives evidence of the important role of IT systems. IT has brought enormous benefits to business and now it can be pointed as a critical part of operation risk effective management [7]. However, the use of IT implies additional risks.

2.2. Operational IT risk management in Latvia

The Latvian Republic integration into the European Union and corresponding rapid economic growth determines the necessity for more effective operational risk management.

The goal of this research is to study operational IT risks as a separate operational risk subgroup from the point of view of monetary and financial institutions, and to develop the operational IT risk management concept within Latvian monetary and financial institutions. This research considers requirements and recommendations of international regulation institutions in the field of financial systems management, such as Basel Committee of the

Bank of International Settlements, Sarbanes-Oxley Act, Financial and Capital Market Commission in Latvia.

It is possible to indicate a set of operational IT risks management problems which are typical for intensively growing Latvian monetary and financial institutions. They are:

- Customer service level decrease due to interruptions of continuous access to IT services
- Demand for qualified IT personnel
- Necessity to modernize information systems software and hardware
- Insufficient IT qualification of information system users
- Inadequate level of existing IT services quality monitoring
- Inadequate level of cooperation between IT specialists and other employees
- Demand for adequate assessment for financial losses resulting from failures or interruptions within information systems
- Demand for IT system development strategic plan, based on a general development plan of monetary and financial institutions
- Inadequate existing IT security level
- Undeveloped strategy of IT system restoration after potential failures and interruptions

These problems indicate the necessity for more complicated IT governance organization. At the same time, the aforementioned requirements and recommendations of international regulation institutions in the field of financial systems management do not pay the necessary attention to the IT subgroup of operational risks as well. As was already pointed, in order to organize successful functioning of monetary and financial institutions, efficient IT risk management has to be realized. Taking into consideration the extreme complexity of IT risk management within the framework of operational risk management system, it is possible to conclude about the necessity to apply international standards of IT governance, such as Information Technology Infrastructure Library (ITIL), Control Objectives for Information and related Technology (CobiT), Code of Practice for Information Security Management (ISO/IEC 27002).

Thus, the development of operational IT risk management system should be based on the requirements and recommendations both in the field of operational risk management and in IT management. It should be noted that applied requirements and recommendations have to correspond with the common priorities and policies of risk management at the corporate level (Figure 2). The COSO (Committee of Sponsoring Organizations of the Treadway Commission) is considered as a generally accepted model of such implementation, whose analysis is not considered in this paper.

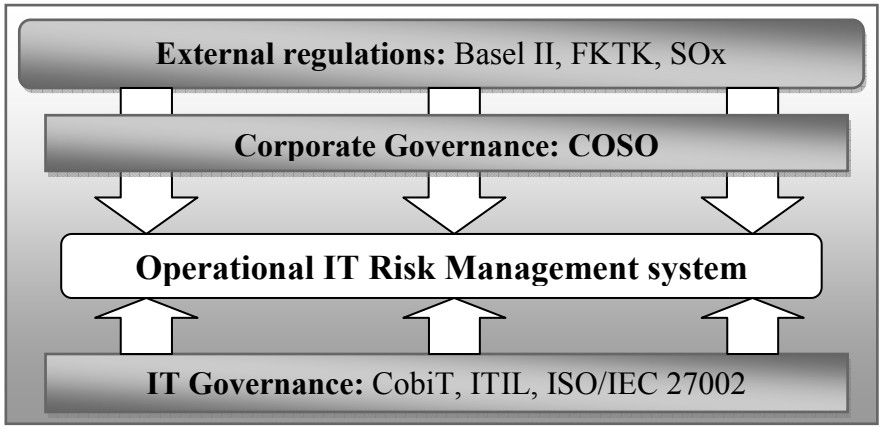

Figure 2. Operational IT risk management system development

3. Requirements to operational IT risk management

First, the common concepts of operational risk management in monetary and financial institutions have to be discussed. As was mentioned above, within this framework the following regulating requirements and recommendations were studied: The Sarbanes-Oxley Act, The New Capital Accord Basel II and Latvian Republic Financial and Capital Market Commission Recommendations for operational risk management.

Public Company Accounting Reform and Investor Protection Act (The Sarbanes-Oxley Act) was accepted in 2002 and became the most wide-ranging legislative act concerning securities, which defines corporate governances rules for monetary and financial institutions.

The International Convergence of Capital Measurement and Capital Standards (The New Capital Accord Basel II), developed by Basel Committee for Banking Supervision, describes banking activity criteria. The advised capital sufficiency measuring and determination methodology is based on the modern theories and practices in developing and functioning of banking activity risk management systems.

Similarly, the Recommendations for operational risk management are developed by The Financial and Capital Market Commission of the Republic of Latvia, where operational risk management principles are summarized. These recommendations should be taken into account by the banks and financial institutions while developing the corresponding operational risk management system.

It should be admitted that these documents specify detailed requirements and recommendations for operational risk management; however, they do not provide any IT governance requirements.

3.1. Requirements of Sarbanes-Oxley Act

Public Company Accounting Reform and Investor Protection Act highlights the fact that the effectiveness of internal controls system is directly dependent on the effectiveness of IT control activities system [9]. 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 [8]:

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

It should be noted that 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.

3.2. Requirements of New Capital Accord Basel II

The purpose of the International Convergence of Capital Measurement and Capital Standards is to increase the reliability and stability of the international banking system. For this purpose the modern risks management technologies should be implemented. New Capital Accord Basel II claims to cardinally modernize bank information systems.

New Capital Accord Basel II requirements, which may correspond to the operational IT risk management, can be listed as follows [7]:

- 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 mitigate material operational risks;
- IT internal audit: operational risk management framework is subject to effective and comprehensive internal audit; conduct regular independent evaluation of a bank's policies, procedures and practices related to operational risks;
- IT ensure continuous service: to have contingency and business continuity plans;
- IT escalation to management: sufficient public disclosure.

3.3. Recommendations of the financial and capital market commission

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 as follows [6]:

- 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).

4. Development of the operational IT risk management concept for Latvian monetary and financial institutions

For developing a concept of operational IT risk management, international IT governance practises have to be reviewed, with a focus on the above mentioned requirements and recommendations for operational risk management. The following documents were reviewed within the current research: Control Objectives for Information and Related Technology (CobiT), IT Infrastructure Library (ITIL) and Code of Practice for Information Security Management (ISO/IEC 27002).

While developing the concept, all operational IT risks identification, classification and assessment have to be focused as high priority tasks in risk management.

4.1. List of IT Governances standards

Control Objectives for Information and Related Technology (CobiT) is developed by IT Governance Institute as a set of documents describing IT governance and audit principles. CobiT precisely formulates governance purposes and principles, management objects, institution's IT processes, its requirements and possible realization approaches [12]. Within IT processes, practical recommendations for IT safety management are discussed as well.

IT Infrastructure Library (ITIL) is one of the most popular approaches to IT governance process organization. ITIL provides a detailed description of important IT division activities, most of which are determined as IT services processes [10].

Code of Practice for Information Security Management (ISO/IEC 27002) is the IT security standard, which is based on risks analysis and management. This standard describes the following aspects: the development of IT security policies; organizational methods of information security ensuring; recourses management; information systems users; communication and processes management; access control; information system acquisition, development and maintenance, information security incident management; business continuity management [11].

5. Operational IT risk management concept for Latvian monetary and financial institutions

As a result of analysis of the above described operational risk management regulating recommendations and existing operational risk management systems in Latvian monetary and financial institutions, the following conceptual requirements of operational IT risk management systems are pointed out:

- to define a strategy for operational IT risk management; the developed strategy should fit a general business-strategy of monetary and financial institutions;
- to find out possible threats to all IT resources, information systems and institution's information;
- based on the conducted analysis of possible IT threats, to identify and classify operational IT risks;
- to develop operational IT risks assessment system, by using both qualitative and quantitative risks characteristics; to apply the developed system for assessment of the risks identified;
- to define methods which can be applied to the operational IT risk management systems and to conduct their assessment as well;
- to develop a policy of most effective methods application for the elimination of defined threats;
- to develop monitoring policy for operational IT risk management system;
- to develop a tool for continuous assessment of applied solutions of operational IT risk management.

For implementation of the above conceptual requirement, it is recommended to use domains, sections and processes from the aforementioned IT governance standards.

Table 1

IT standards determination

Requirements	Domains, sections and processes
Operational IT risk management strategy determination	• CobiT. PO1. Define a strategic IT plan; PO4. Define the IT Organisation and Relationships; ME4. Provide IT Governance • ITIL. Service Strategy. 4. Service strategy; 7. Strategy, tactics and operations. Service Design. 4.6. Information Security Management • ISO/IEC 27002. 4. Risk assessment and treatment; 5.1. Establish an information security policy; 6.1. Establish an internal security organization; 8.1. Emphasize security prior to employment; 15.1. Comply with legal requirements
IT threats determination	• CobiT. PO9. Assess and Manage IT Risks • ITIL. Service Strategy. 9.5. Risks. Service Design. 4.5.5. Process activities, methods and techniques. Service Transition. 9. Challenges, critical success factors and risk. Continual Service Improvement. 5.6.3. IT Service Continuity Management • ISO/IEC 27002. 5.1. Establish an information security policy; 13.1. Report security events and weaknesses; 14.1. Use continuity management to protect information
Operational IT risk identification	• CobiT. PO9. Assess and Manage IT Risks • ITIL. Service Strategy. 9.5. Risks. Service Transition. 9. Challenges, critical success factors and risk. Continual Service Improvement. 5.6.3. IT Service Continuity Management • ISO/IEC 27002. 5.1. Establish an information security policy; 12.1. Security requirements analysis and specification; 13.1. Report security events and weaknesses
Operational IT risk assessment system development	• CobiT. PO9. Assess and Manage IT Risks • ITIL. Service Strategy. 9.5. Risks. Service Transition. 4.6. Evaluation • ISO/IEC 27002. 5.1. Establish an information security policy; 12.1. Security requirements analysis and specification
Defining methods for operational IT risk management	• CobiT. PO9. Assess and Manage IT Risks • ITIL. Service Strategy. 9.5. Risks. Service Design. 3.4. Identifying and documenting business requirements and drivers. Service Transition. 4.6. Evaluation • ISO/IEC 27002. 5.1. Establish an information security policy; 12.1. Security requirements analysis and specification; 13.1. Report security events and weaknesses
Policy development for risk management most effective methods	• CobiT. PO10. Manage Projects; DS4. Ensure continuous service • ITIL. Service Design. 3.5. Design activities; 4.5. IT Service Continuity Management; 4.6. Information Security Management. Service Transition. 3.2. Policies for Service Transition • ISO/IEC 27002. 5.1. Establish an information security policy; 6.1. Establish an internal security organization; 10.5. Establish backup procedures; 14.1. Use continuity management to protect information
Risk management system monitoring policy development	• CobiT. PO10. Manage Projects; ME1. Monitor and evaluate IT performance; ME2. Monitor and evaluate internal control; AI7. Install and accredit solutions and changes • ITIL. Service Strategy. 4.4. Prepare for execution. Service Design. 3.5. Design activities; H. The service management process maturity framework. Service Transition. 3.2. Policies for Service Transition. Service Operation. 5.1. Monitoring and control • ISO/IEC 27002. 6.1. Establish an internal security organization; 8.2. Emphasize security during employment; 10.10. Monitor information processing facilities; 12.4. Protect and control system files; 12.5. Control development and support processes
Development of techniques for regular assessment of risks management system quality	• CobiT. ME4. Provide IT Governance; DS4. Ensure continuous service • ITIL. Service Strategy. 3.1. Value creation; 4.4. Prepare for execution; 9.4. Effectiveness in measurement. Service Design. 3.6. Design aspects; 3.10. Business service management; 4.5. IT Service Continuity Management; 4.6. Information Security Management. Continual Service Improvement. 4.3. Service measurement • ISO/IEC 27002. 5.1. Establish an information security policy; 6.1. Establish an internal security organization; 10.5. Establish backup procedures; 14.1. Use continuity management to protect information

4. Conclusions

The extension of Latvian monetary and financial institutions asks for more intensive attention to operational risks management. Herewith, most operational risks depend on the applied information technology whose governance reduces the general level of operational risks.

In the current paper, a management concept of operational IT risk as a separate operational risk subgroup is developed. The conducted analysis of existing operational risks management practices indicates insufficient level of operational IT risk management requirements. So, while developing the concept, recommendations and requirements of international regulation institutions in the field of financial management system should be taken into consideration as well as international standards for IT governance.

The development of operational IT risk management technique based on the concept discussed above can be considered an enhancement of the current research.

References

1. Jordan E., Silcock L. Beating IT Risks // John Wiley & Sons, Ltd, 2005.
2. King J. Operational Risk: Measuring and Modelling // John Wiley & Sons, Ltd, 2001.
3. Moosa I. Operational Risk Management // Antony Rowe Ltd, Chippenham and Eastbourne, 2007.
4. Walker S. Operational Risk Management: Controlling opportunities and threats // Connley Walker Pty Ltd, 2001.
5. International Convergence of Capital Measurement and Capital Standards: A Revised Framework // Basel Committee for Banking Supervision, 2004.
6. Recommendations for Operational Risk Management // Latvian Republic Financial and Capital Market Commission, 2006. (in Latvian)
7. IT Control Objectives for Basel II. The Importance of Governance and Risk Management for Compliance // IT Governance Institute, 2007.
8. IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control over Financial Reporting // IT Governance Institute, 2006.
9. Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley Act) // US Federal Law, 2002.
10. The Office of Government & Commerce. ITIL Lifecycle Publication Suite: Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement // The Stationery Office, 2007.
11. ISO/IEC 27002. Information Technology - Security Techniques - Code of Practice for Information Security Management // ISO/IEC, 200.
12. CobiT 4.1 // IT Governance Institute, 2007.

Kļimovs Ruslans, Rezniks Aļberts, Solovjova Irina un Šlihte Jans. Operacionālo informācijas tehnoloģijas risku pārvaldības koncepcijas izstrāde

Mūsdienu apstākļos operacionālo risku vadība un IT pārvaldība tiek atzīta par monetāro un finanšu iestāžu augstāko uzņēmējdarbības prioritāti. Tajā pašā laikā informācijas tehnoloģiju augstā ievainojamība var izraisīt

lielus finansiālus zaudējumus. Savukārt pasaules regulējošo iestāžu prasībās un rekomendācijās nav noteiktas prasības operacionālo risku vadībā izmantojamām informācijas tehnoloģijām. Šis pētījums izvirza operacionālus IT riskus par operacionālo risku svarīgu apakšgrupu, kuras pārvaldība pazemina operacionālo risku kopējo līmeni. Līdz ar to tika izpētīti šādi operacionālo risku vadības un IT pārvaldības dokumenti: The Sarbanes-Oxley Act, The New Capital Accord Basel II, Latvijas FKTK operacionālo risku vadības ieteikumi, ITIL, CobiT un ISO/IEC 27002. Balstoties uz šiem teorētiskiem pētījumiem, tika izstrādāta operacionālo IT risku pārvaldības koncepcija.

Klimov Ruslan, Reznik Albert, Solovjova Irina and Slihte Jans. The development of the operational IT risk management concept

Nowadays the governance of information technology and operational risk management are the highest business activity priorities for monetary and financial institutions. Information technology can be pointed as a vulnerable area, which can be affected by dire financial consequences. Still, currently used recommendations and requirements of international regulation institutions do not provide certain IT requirements to operational risk management. This research discusses operational IT risks as an important operational risks subgroup whose management reduces the general level of operational risks. Thus, the following operational risks management and IT governance standards are reviewed: The Sarbanes-Oxley Act, The New Capital Accord Basel II, Latvian FCMC Recommendations for Operational Risk Management, ITIL, CobiT and ISO/IEC 27002. Based on these theoretical researches, the concept of the operational IT risk management is developed.

Климов Руслан, Резник Альберт, Соловьева Ирина и Шлихте Янс. Разработка концепции по управлению операционными рисками в информационных технологиях

Управление операционными рисками и стратегическое управление информационными технологиями в современных условиях становится важнейшим бизнес-приоритетом монетарных и финансовых учреждений. В то же время, высокая уязвимость информационных технологий может привести к большим финансовым потерям. Однако требования и рекомендации международных регулирующих учреждений, применяемые в настоящее время, не определяют конкретные требования к применяемым информационным технологиям в управлении операционными рисками. Данное исследование как важную подгруппу операционных рисков рассматривает операционные ИТ-риски, стратегическое управление которыми значительно уменьшает общий уровень операционных рисков. В связи с этим, были изучены следующие документы в областях управления операционными рисками и стратегического управления информационными технологиями: The Sarbanes-Oxley Act, The New Capital Accord Basel II, латвийские рекомендации по управлению операционными рисками, ITIL, CobiT и ISO/IEC 27002. Основываясь на этих теоретических исследованиях, была разработана концепция стратегического управления операционными ИТ-рисками.