A Technique for Operational IT Risk Management in Latvian Monetary and Financial Institutions

ANDREJS ROMANOVS, YURI MERKURYEV, RUSLAN KLIMOV
Department of Modeling and Simulation
Riga Technical University
Riga, Kalku str. 1
LATVIA

IRINA SOLOVJOVA
Department of Finances
University of Latvia
Riga, Aspazijas blvd. 5
LATVIA

Abstract: - The existing operational risk management systems do not always adequately recognize risks connected with informational system application. Conducted analyse of Latvian monetary and financial institutions points on the inadequate level of IT risk management within operational risks management system. Thus, this research considers the problem of IT risks as operational risks subgroup, for which management, IT governance standards and practices should be used. Finally, the paper presents the technique for operational IT risks management system development for use within Latvian monetary and financial institutions.

Key-Words: - operational risks, risk management, IT governance

1 Introduction
The Latvian Republic integration into the European Union and corresponding economic growth determines the rapid extension of monetary and financial system. Due to the increased intensity of performed financial operations, monetary and financial institutions became very vulnerable to operational risks. In many cases, the high level of operational risks is conditioned by IT system failures. The conducted analyse of Latvian monetary and financial institutions points the inadequate level of IT risk management within operational risks management system. The current situation indicates the necessity for more complicated IT governance organization and more effective operational IT risk management system development. This research analyzes IT risks as a separate operational risk subgroup. Our previous paper [1] discussed the operational IT risk management concept, which is based on requirements and recommendations of international regulation institutions in the field of monetary and financial system management. At the same time, the concept insists on application of modern IT governance standards and practices. Thus, the next goal for this research is to develop technique, which provide more detailed description about operational IT risk management procedures and to specify IT governance standards and practices, which should be realized with the purpose to realize this technique in Latvian monetary and financial institutions.

2 Concept
As it was mentioned, this research considers operational IT risks as the separate operational risk subgroup and advises separate concept for these risks management. According to this concept, following international operational risks management regulation in the field of financial systems should be considered:
- Basel Committee of the Bank of International Settlements;
- Sarbanes-Oxley Act;

Then, requirements and recommendations, which may correspond to the operational IT risk management, should be pointed.

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 [5]. 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 [7]:

- 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.

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. 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 [4]:

- 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; 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.

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 [8]:

- 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).

At the same time, the aforementioned requirements and recommendations 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 and practices of IT governance, such as:

- Information Technology Infrastructure Library;
- Control Objectives for Information and related Technology;
- Code of Practice for Information Security Management.
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 [2]. 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 [9].

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 [6].

![Diagram](image)

**Fig. 1: Operational IT risk management concept**

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 (see Figure 1). The COSO (Committee of Sponsoring Organizations of the Treadway Commission) is considered as a generally accepted model of such implementation. Still, here it is stated that the corporate governance specification should be applied within the implementation of operational IT risk management system. Thus, corporate governance model and applications are not analyzed in this research.

### 3 Technique

As a result of analysis of the aforementioned operational risk management regulating recommendations and existing operational risk management systems in Latvian monetary and financial institutions, a technique for operational IT risk management has been developed that is based on the previously published concept [1].

The technique consists of the following six stages:

1. Analyze the current operational risk management system:
   - Determine a strategy of operational IT risk management;
   - Analyze the existing information system of an institution.

2. Identify operational IT risks
   Determine potential threats to IT systems and projects:
   - threats to IT resources (information and technologic processes resources);
   - threats to information system (during IS development and implementation; during IS application and support; during IS modifications);
   - threats to information (confidentiality violation, unauthorized modifications, failures and losses, and access violations).

3. Classify operational IT risks
   Classify identified operational IT risks:
   - determine tasks and criteria for classification of threats to IT resources, threats to information systems, and threats to information;
   - perform classification of operational IT risks in accordance with the stated tasks and determined criteria.

4. Assess operational IT risks
   Perform classified risk assessment, considering the current situation and the applied IT security policy:
   - Assess all risks during a particular period of time. It is permitted to use statistical data available and experience of appropriate specialists for risk assessment;
• Assess the probability of occurrence for all risks within a particular period of time, using the following quality levels:
  • improbability of the given threats
  • low probability of the given threats occurrence
  • significant probability of the given threats occurrence
  • high probability of the given threats occurrence
• Assess the influence of all institutions IS risks within a particular period of time. When it is possible, determine the values of this influence for further quality determination of resources that are necessary for restricting risk influence;
• Assess impact of all risks on institutions IS within a particular period of time by application of the following quality levels:
  • no negative impact
  • insignificant impact
  • significant impact
  • crucial impact
• Determine and calculate criteria of complex risk assessment based on the parameters of impact and occurrence probability of identified threats, with the aid of mathematical methods.

5. Realize operational IT risk management system
• identify a set of potential solutions for identified risks management;
• assess the identified solutions using specified criteria;
• select best solutions for the management of each risk, based on the assessment of risk, performed earlier, and possible solutions.

6. Monitor operational IT risk management system
• implement monitoring mechanism for the effective implementation of the strategy;
• determine a set of tasks, whose solution does not satisfy the requirements of the operational IT risk management strategy.

4 Domains, sections and processes
The previous section describes basic stages for operational IT risk management system realization. It should be admitted again that advised technique is based on existing international recommendations and requirements of operational risk management. Thus, in our research, the main attention is directed to risk identification, classification and assessment phases (technique stages 2, 3 and 4 are described in more detail), which are described inadequately in these documents. At the same time, the advised concept advises IT governance processes implementation while operational IT risk management technique realization (see Figure 2).

Fig. 2: Technique development

Thus, in the current section, domains, sections and processes of IT governance standards and practices, which correspond to separate phases of the developed technique, are advised.

At the first stage “Analyze the current operational risk management system” it is possible to use the following domains, sections and processes of IT governance standards and practices:
• CobiT. PO1.3 “Assessment of current capability and performance”; PO1.4 “IT strategic plan”; PO1.5 “IT tactical plans”; PO4.1 “IT process framework”; PO4.5 “IT organisational structure”; ME4.2 “Strategic alignment”; ME4.4 “Resource management”; ME4.5 “Risk management”;

4 Domains, sections and processes
The previous section describes basic stages for operational IT risk management system realization. It should be admitted again that advised technique is based on existing international recommendations and requirements of operational risk management. Thus, in our research, the main attention is directed to risk identification, classification and assessment phases (technique stages 2, 3 and 4 are described in more detail), which are described inadequately in these documents. At the same time, the advised concept advises IT governance processes implementation while operational IT risk management technique realization (see Figure 2).

Thus, in the current section, domains, sections and processes of IT governance standards and practices, which correspond to separate phases of the developed technique, are advised.

At the first stage “Analyze the current operational risk management system” it is possible to use the following domains, sections and processes of IT governance standards and practices:
• CobiT. PO1.3 “Assessment of current capability and performance”; PO1.4 “IT strategic plan”; PO1.5 “IT tactical plans”; PO4.1 “IT process framework”; PO4.5 “IT organisational structure”; ME4.2 “Strategic alignment”; ME4.4 “Resource management”; ME4.5 “Risk management”;

4 Domains, sections and processes
The previous section describes basic stages for operational IT risk management system realization. It should be admitted again that advised technique is based on existing international recommendations and requirements of operational risk management. Thus, in our research, the main attention is directed to risk identification, classification and assessment phases (technique stages 2, 3 and 4 are described in more detail), which are described inadequately in these documents. At the same time, the advised concept advises IT governance processes implementation while operational IT risk management technique realization (see Figure 2).

Thus, in the current section, domains, sections and processes of IT governance standards and practices, which correspond to separate phases of the developed technique, are advised.

At the first stage “Analyze the current operational risk management system” it is possible to use the following domains, sections and processes of IT governance standards and practices:
• CobiT. PO1.3 “Assessment of current capability and performance”; PO1.4 “IT strategic plan”; PO1.5 “IT tactical plans”; PO4.1 “IT process framework”; PO4.5 “IT organisational structure”; ME4.2 “Strategic alignment”; ME4.4 “Resource management”; ME4.5 “Risk management”;

4 Domains, sections and processes
The previous section describes basic stages for operational IT risk management system realization. It should be admitted again that advised technique is based on existing international recommendations and requirements of operational risk management. Thus, in our research, the main attention is directed to risk identification, classification and assessment phases (technique stages 2, 3 and 4 are described in more detail), which are described inadequately in these documents. At the same time, the advised concept advises IT governance processes implementation while operational IT risk management technique realization (see Figure 2).

Thus, in the current section, domains, sections and processes of IT governance standards and practices, which correspond to separate phases of the developed technique, are advised.

At the first stage “Analyze the current operational risk management system” it is possible to use the following domains, sections and processes of IT governance standards and practices:
• CobiT. PO1.3 “Assessment of current capability and performance”; PO1.4 “IT strategic plan”; PO1.5 “IT tactical plans”; PO4.1 “IT process framework”; PO4.5 “IT organisational structure”; ME4.2 “Strategic alignment”; ME4.4 “Resource management”; ME4.5 “Risk management”;
At the second stage “Identify operational IT risks” it is possible to use the following domains, sections and processes of IT governance standards and practices:

- **CobiT.** PO9.2 “Establishment of risk context”; PO9.3 “Event identification”;

At the third stage “Classify operational IT risks” it is possible to use the following domains, sections and processes of IT governance standards and practices:

- **CobiT.** PO9.1 “IT risk management framework”; PO9.3 “Event identification”; PO9.4 “Risk assessment”;

At the fourth stage “Assess operational IT risks” it is possible to use the following domains, sections and processes of IT governance standards and practices:

- **CobiT.** PO9.4 “Risk assessment”; PO9.5 “Risk response”;
- **ITIL. Service Strategy.** 9.5. “Risks”; **Service Transition.** 4.6. “Evaluation”;

At the fifth stage “Realize operational IT risk management system” it is possible to use the following domains, sections and processes of IT governance standards and practices:

- **CobiT.** PO9.6 “Maintenance and monitoring of a risk action plan”; PO10.2 “Project management framework”; PO10.3 “Project management approach”; PO10.5 “Project scope statement”; PO10.8 “Project resources”; A17. “Install and accredit solutions and changes”; DS4.3 “Critical IT resources”;

At the sixth stage “Monitor operational IT risk management system” it is possible to use the following domains, sections and processes of IT governance standards and practices:

- **CobiT.** PO10.10 “Project quality plan”; PO10.11 “Project change control”; PO10.13 “Project performance measurement, reporting and monitoring”; A17.9 “Post-implementation review”; DS4. “Ensure continuous service”; ME1. “Monitor and evaluate IT performance”; ME2. “Monitor and evaluate internal control”; ME4.4 “Resource management”; ME4.6 “Performance measurement”;

5 Conclusions
In this paper the problem of operational IT risks management is discovered. Within analysis of operational risks management requirements and recommendations for monetary and financial institutions, following documents were studied: “Public Company Accounting Reform and Investor Protection Act”, “International Convergence of Capital Measurement and Capital Standards” and Latvian FCMC “Operational risk management recommendations”. The conducted analysis indicates inadequate management of risks in the IT field. Thus, the technique for operational IT risk management was developed based on previously designated concept, according to which, IT governance standards and practise was applied to operational risk management. The developed technique is intended for application in Latvian monetary and financial institutions, what is the goal for further research.

References: