Methodology for Designing Operational Banking Risks Monitoring System

T N Kostjunina

Saint Petersburg State University of Architecture and Civil Engineering, 4 Vtoraya Krasnoarmeyskaya Str., Saint Petersburg, 190005, Russia

E-mail: tnktn@yandex.ru

Abstract. The research looks at principles of designing an information system for monitoring operational banking risks. A proposed design methodology enables one to automate processes of collecting data on information security incidents in the banking network, serving as the basis for an integrated approach to the creation of an operational risk management system. The system can operate remotely ensuring tracking and forecasting of various operational events in the bank network. A structure of a content management system is described.

1. Introduction
Issues of banking risk management are currently becoming crucial for financial institutions. As banking operations become more complex and their number increases, the success of banking business and bank’s ability to improve its performance depend primarily on how quickly and timely the bank manages possible threats and risks.

The computerization of banking operations made it possible to introduce new financial technologies and significantly improve the performance of bank employees. However, the introduction of information technologies contributed to new issues in banking business. Currently, bank information systems and technologies are one of the reasons for the formation of various operational risks. The first works dedicated to the analysis and evaluation of this type of risk have appeared relatively recently. Only in the 1990s, banking institutions started to recognize risks related to rapid growth of automation in their business, in particular, an insufficient management of confidential information, software errors and mistakes of employees when entering data, fraud using information systems, failures of software and hardware followed by business interruption, risk of data loss. Currently, design of an operational risk management system represents a challenge for any bank.

2. Bank operational risks: key concepts
At the present time, consulting companies, banks and international institutions are actively designing practical aspects of risk management. Guidelines of the Basel Committee on Banking Supervision serve as the basis for such activities [1].

No definite understanding of operational risk has been developed in the modern economics literature yet which results in different interpretations of the essence of this risk type and ways of its management.

In 2001, the Basel Committee proposed defining operational risk as follows: operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

Risks, including operational ones, are classified based on selected criteria. They may be: sources of origin, field of risks, credit institution business nature, etc. Let us review a classification of bank operational risks depending on their origin, with the definition of bank operational risk, provided in Basel Committee documents, taken as the basis [2,3,4].
1. Personnel risks: risk of incompetence in employees engaged in the operation; risk of careless duty performance (non-compliance with the established rules, procedures and regulations); risk of personnel overload; risk of lack of qualified or key employees at a specific site; risk of accidental single errors; other risks related to personnel specifics or HR management processes.

2. Risks of information systems: risks of equipment failure (ATMs, computer and telecommunications hardware, etc.); risks of software failure or malfunction; risk of information loss or leakage.

3. Technological risks: risk of a faulty bank’s organizational structure resulting in overlapping or non-fulfillment of certain types of functions; risk of an incorrectly introduced (faulty) methodology for process implementation; legal risk in terms of non-compliance of bank’s contractual and internal documents with the current legislation, which results in the imposition of fines or sanctions on the bank.

4. Risk of external influence on internal bank facilities, processes, and technologies: risk of unauthorized access to bank processes (electronic databases, archives, depository, bank premises, etc.); risk of theft of specific types of assets; risk of accidents or adverse external events (natural, man-induced, social, political, etc.).

3. Creation of an operational banking risks monitoring system

The purpose of operational risk management is to maintain the risk assumed by the bank at the level determined by the bank according to its strategic objectives. The priority is to ensure the maximum safety of assets and capital through reduction (elimination) of possible losses.

In terms of a systemic approach, operational risk management is a continuous process based on the following steps: risk identification; risk assessment; risk monitoring; making decisions on risk management. Operational risk monitoring is crucial in this sequence.

Normally, the system of operational risk level indicators is used for monitoring. Those are indicators that are theoretically or empirically related to the level of operational risk assumed by the bank. The following can be used as operational risk level indicators: the number of failed or incomplete banking operations; the number of dismissed (resigned) employees; the number of errors made during operations; the number of accidents, failures of information technology systems; downtime of information technology systems, etc.

To date, foreign banks have gathered solid experience in applying key risk indicators (KRI) which play a significant role in management of any risks. The indicators are used to monitor and predict various operational events.

In managing operational risks, key risk indicators are the main tools which allow performing a wide range of measurements. Unlike audits and control activities which take place regularly, key risk indicators can be measured as often as required (daily, monthly, etc.).

The monitoring system should automate the following steps: collection of risk and loss occurrence facts; events typification; evaluation of events occurred; elaboration of key risk indicators; testing of key risk indicators using the expert evaluation method; entering data on company employees; receiving a report on estimated risk.

In the course of system creation, data modules (entering/editing/deleting data on events that took place in the company), and a decision-making module, which is used to define business processes representing potential operational risk carriers, should be developed. The developed modules are used to automate the process of operational risks monitoring.

For flexible application of the system for monitoring operational banking risks, web-technologies were selected allowing one to work in the information system remotely without being bound to any particular place.

The first step in the system creation is to elaborate use cases. A use case describes typical interaction between the user and the system and demonstrates the system behavior from the user's perspective. At the basic level, a use case is determined while discussing with the user functions to be implemented or goals pursued in relation to the system being developed [6].

Elaboration of a use case model includes the following steps:

- selecting actors;
- selecting use cases;
- developing a use case model.

Use of case diagrams illustrate users’ requirements (in the form of user/system interaction scenarios).

4. System actors

In banks, to differentiate access rights, different individuals perform data input and output.

The main actors in the operational risk monitoring system being developed are the following:

- user;
In order to record functional requirements to the system, general use case diagrams were constructed using the Rational Rose environment (Fig. 1).

Let us review the needs of each actor.

The user needs to: register in the system; record an event; view the event log; access user account.

The risk coordinator has the same needs as the user plus one more: typification of the events occurred.

The risk manager has the same needs as the user plus several more: evaluating event consequences; managing Key Risk Indicators (KRI).

The expert needs to: log in to evaluate the KRI selected by the system.

The administrator, in addition to user's basic functions, needs to: confirm registration; edit the event log; edit the data on employees.

Functional requirements are represented by the use case model. Interaction scenarios were developed for detailed recording of the actor/system interaction process as a part of the use case.

Figure 1 shows a use case diagram as a concept of a business system.

Figure 1. Use case diagram

Use case diagrams are the most common representation of functional requirements to the system. Further system designing requires more specific details which are described in a document called a “use case scenario” or “flow of events”. The scenario records in details the actor/system interaction process implemented as a part of the use case.

Based on tasks assigned to the system, the following interfaces were developed: administrator, bank's risk manager, bank's risk-coordinator, system user and expert interfaces.
In general, the content management system structure regarding the created WEB-portal module is shown in Fig. 2.

**Figure 2.** Content management system structure

5. Conclusion
The issue of risk management in banks is critical, as a wrong approach to this issue may not only result in large losses, but also lead to closure of such financial institution. This explains the necessity and urgency of establishing systems for monitoring operational banking risks.

The web-based system for monitoring operational banking risks of a financial institution includes the management procedure for collection and consolidation of data on actual losses incurred by the financial institution as a result of operational risks.

Only employees of the financial institution shall have access to the system. Anyone can create an account in the system; however, to take full advantage of the system functions, an administrator’s permission is required. The administrator provides access to the system adding a user to a particular group with appropriate rights.
References

[1] Basel Committee on Banking Supervision. *Operational Risk — Supervisory Guidelines for the Advanced Measurement Approaches*, June 2011

[2] Sazykin B V 2007 *Upravlenie operatsionnym riskom v kommercheskom banke*. (M.: Izd-vo «Vershina»)

[3] Lavrushina O I, Valentsevoi N I 2007 Bazel'skie prin-tsipy effektivnogo (M.: KNORUS)

[4] Shapelle A, Crama Y, Hübner G, Peters J P 2008 Practical methods for measuring and managing operational risk in the financial sector: a clinical study. *Journal of Banking and Finance* 32 1049–1061

[5] Kostjunina T N 2011 *Simulation of operational bank risks X international scientific-practical conference «ACTUAL PROBLEMS OF ECONOMY AND NEW TECHNOLOGIES OF TEACHING». Vol. 3.* (ST.-PETERSBURG)

[6] Kostjunina T N 2011 *Verojatnostnoe modelirovanie operacionnych bankovskich riskov*. (SPb, IBI)

[7] Gamza V A 2011 *Bezopasnoct bankovskoy deyatelnosti*. (M.: Market)

[8] Frost C, Allen D, Porter J, Bloodworth P 2000 *Operational risk and resilience: Understanding and minimizing operational risk to secure shareholder value*. (Oxford: ButterworthHeinemann)

[9] Oh J C, Yun E, Golkovski M G and Lee S 2003 *Mater. Sci. Eng. A* 351 98-108

[10] Carol A 2003 *Operational Risk: Regulation, Analysis and Management* (Pearson Education, FT Prentice Hall)