Operational Risk Management in Business Processes

Alexander Gromoff¹, Julia Stavenko², Kristina Evina³ and Nikolay Kazantsev⁴

¹,²,³,⁴National Research University Higher School of Economics, Faculty of Business Informatics, BPM Department, Science & Education Center of Information Control Technologies, Moscow, Russia
E-mails [alexander.gromoff@me.com, kevina@convera.ru, {ystavenko, nkazantsev}@hse.ru]

Abstract: The article is dedicated to a problem of realizing operational risk management in a real-life environment of a business process organization, when classic methods of operational risk management, based on statistics, could not be used or are ineffective. The given research was held in the context of the contract № 13.G25.31.0096 with the Ministry for Education and Science of Russian Federation «Deployment of hi-tech manufacture of unstructured information processing in cross-platform system on the free software basis due to increase management efficiency of innovative activity of the enterprises in the modern Russia economy»

Keywords: operational risk management, reactive and active risk management, proactive risk management, risk owner, quantitative assessment, operational risk exposure, expected and unexpected losses, subject-orientated modeling and process management
1. Introduction

Operational risk management (ORM) is attracting more and more attention of governmental and commercial organizations worldwide due to an increasing amount of outstanding operational losses (that are impossible to predict due to the absence of ORM policies), as well as due to unexpectedness and fluctuations (instability) of the external business environment. As a respond to this problem the Basel Committee on Banking Supervision (BCBS) has released a new standard\(^1\), where the main methods of operational risk appraisal in banks were formulated. An operational risk (OR) was defined as: «a risk of losses influenced by (1)drawbacks or errors in the execution of internal processes made by employees, running IT systems and technologies; as well as due to (2)external events, and also (3)juridical risk». According to the standard requirements, banks and then organizations in other economy branches have started to implement the process of ORM in companies.

ORM is a metaprocess integrated into all enterprise architecture components: into business processes, information flows, IT Infrastructure. Like a typical process of continuous improvement, ORM process has a cycle repeatable nature, and is a variation of PDCA cycle\(^2\):

- Definition of enterprise business context (the mission, strategic objectives, risk appetite);
- Identification of operational risks;
- Qualitative and quantitative analysis (e.g. in banks – capital reservation for OR);
- ORM strategy implementation;
- Control and monitoring of ORM strategy implementation.

The main problem here is that companies perceive ORM process implementation as a sequence of individual tasks, like the definition of weakest control links (procedures), development of planning initiatives, collection of loss databases, calculation of capital reserved for operational risks and etc. In fact, these actions are a response to the requirements of Sarbanes-Oxley, COSO, ISO 9000 and Basel II. Thereby, substantial sums of money are invested in risk management programs, and afterwards they not paid out by achieved results. Many companies disappointed by a lack of results have come to the mistaken conclusion that ORM is another ineffective initiative, which is necessary for the sake of appearance. Such a mistaken opinion is mostly caused by applying ORM methods incorrectly as well as by displaying or fully ignoring strategic planning or, in other words, strategy-supportive risk culture. The most common mistakes are as follows:

- misalignment between the chosen ORM strategy and risk appetites of different stakeholders,
- application of internal control procedures, audit and insurance without integrating ORM into a business architecture,
- ORM within departments and lack of transparency in the control and standardization process (a silo approach),
- risk identification by adopting the “top-down” approach alone: risks are grouped in accordance with the classification, afterwards they are thoroughly analyzed to build a risk map (measurement of a likelihood of risk occurrence and potential losses),
- evaluation of overall influence of risks based on the risk map, creation of a system of key risk indicators for analyzing the evolution of OR influence and monitoring risks.

As a result, a risk is identified when income losses have already been incurred or given the already known risk factors, risk monitoring is carried out in nearly real-time mode (reactive and active OR management).

On the one hand, the «top-down» approach described above seems to be adequate and correct, however companies are not immune to substantial losses caused by uncontrollable risks: operational risks are identified, however they are not controlled or controlled post factum. That has lead to a revision of existing approaches to ORM in order to create an effective collaboration in specialized departments or groups, dealing with the identification and control of risk occurrence in business processes and describing OR in accordance with the «bottom-up» approach.

The «bottom-up» approach implies that factors of risk occurrence and its effects are appraised on the level of distinct departments in an interactive way by evaluating responses of employees, processes, technologies on internal and external impacts, i.e. proactive ORM is realized (the possible reason of a risk is identified and eliminated). Without denying the measurement and description of risks with the help of centralized ORM, this approach classifies operational risks within functional lines or introduces an integrated approach to measuring risks in processes that is based on expert judgments and quantitative methods.

---

\(^1\) new Basel Capital Accord  
\(^2\) Plan do check act
Thus, the formal «top-down» approach enables a sequential application of standard risk management methods, while self-appraisal of risk exposure made by distinct business units in accordance with the «bottom-up» approach strengthens business areas that are actually risk owners.

2. Integration operational risk management into business architecture

In the last few years it became clear that, despite the implementation of the «bottom-up» approach to ORM, companies incur losses due to risks of an external environment (an unexpected enactment of new laws and regulations by the government, unforeseen changes of a business situation) as well as due to a low speed of implementing OR control measures, i.e. due to the low flexibility and adaptation of business processes to changes.

In order to implement ORM into business operations of the company and to achieve strategic goals in line with risk appetite, it is essential to implement ORM into all components of enterprise architecture in changing business conditions.

This integration ensures strategic and operational resilience of the company’s business (i.e. a capability of systems, resources, processes effectively supports the business in case of unforeseen risks) due to maintaining an acceptable level of OR and due to an optimal for company’s owners balance between profit maximization and long-term business stability.

How can this integration be achieved in practice? The idea of ORM lies in ensuring a required quality of all operations and processes, therefore the optimal way for implementing ORM is an integrated documentation of all company’s business processes while simultaneously highlighting bottlenecks as potential risk sources in each of them (so called “points of income losses”), business process automation along with a constant monitoring of risk indicators and taking control measures, analysis of results and control for making a decision about business process or ORM strategy modification. Meanwhile, costs necessary for assessing, minimizing and controlling risks should not exceed profitability of a process itself.

The question emerges how to accomplish this integration in practice. There are several principles of risk management:

1. principle of complexity – cooperation of all company’s departments in identifying and evaluating risks in each line of business.
2. principle of continuity – continuous monitoring and control of company’s risks, since conditions in which the organization is running constantly change, new risks emerge and a thorough analysis and control of them are required.
3. principle of integration – need to give a balanced evaluation of the impact of the entire spectrum of risks on business, ranging from a possible reduction of product prices to potential losses caused by technological accidents.

Business process management is a cyclic process as well; therefore, it is necessary to align phases of ORM process with phases of business process management.

Integration of ORM process into business process execution is characterized by a rate of completeness (to what extent ORM processes cover all systems, products and processes that exist in the company and might be sources of revenue losses) and a rate of responsiveness (how quickly the transition from a reactive phase of risk solving to an active one and probably to a proactive phase takes place). In order to ensure a correspondence between these rates and the level of risk appetite in the organization, it is necessary to have a flexible instrument of business process management, in which the process of managing a new OR should move from the reactive phase (detection of losses, examination, removal) via the active one (monitoring, removal) towards the proactive stage (avoidance).

Subject-oriented approach is a new and cutting edge in terms of adaptability requirements method of documenting and modeling business processes, where process participants are the focus of attention. This approach was realized in the product Metasonic Suite, which consists of three modules: the module Metasonic Build allows modeling of organization’s processes, Metasonic Proof was developed for validating process models, the module Metasonic Flow allows to directly execute a process.

3. Realizing the task of operational risk management by way of example of delivery process

2.2. Phase 1

Let’s take the process of order delivery in an online store as an example.

In accordance to the shown methodology, the phase of setting an environment for business process management comprises a definition of risk management context, which refers to a set of internal and external factors (conditions), in which ORM takes
place. This process involves the analysis and review of strategic corporate goals, strategic plans, initiatives (campaigns) and metrics in order to define main parameters (boundaries) within which it is necessary to manage risks. The context also includes an internal and external environment of the company.

At this phase fundamental documents, such as a strategic plan, business plans and budgets, annual reports, economic analyses and other documentation containing registered company information are used. Also, in the course of defining risk management context it is necessary to comply planned results of business process and identified boundaries of risk management process with the current legislation.

Regarding the order delivery process the company sets the following strategic goal: to decrease the amount of refused client to 5%. This goal will be the backbone for identifying risks within the delivery process and will be a guideline while defining causes and factors of risk situation occurrence.

**Phase 2**

*The modeling phase* comprises a detection and evaluation of OR, i.e. a process is analyzed in order to detect steps, where a mistake might lead to failures (mistakes of planning, realization, verification, representation, data transfer, selection are considered), the nature of detected mistakes is determined; possible compensation actions are defined and preventive measures are formulated.

Table 1 contains the assessment results of identified risks for the function «Customer calling»:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Likelihood of occurrence</th>
<th>Factors of OR</th>
<th>Preventive measures against the problem (the major problem)</th>
<th>Control measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>A client has refused</td>
<td>13.66%</td>
<td>A client has refused an «expensive» order.</td>
<td>Set high priorities for expensive orders, call a client in the first place</td>
<td>Setting a higher priority for the order, offering bonuses, discounts etc. by the operator</td>
</tr>
<tr>
<td>A client has not been reached by a telephone till the end of a marketing campaign</td>
<td>5.49%</td>
<td>A client is not reachable for confirming an order during a marketing campaign until its end. The order is cancelled.</td>
<td>SMS sending, notifying about an upcoming telephone call; e-mail sending (e.g. with a link for order confirmation), optimization of call-center operation (increase of frequency of telephone calls).</td>
<td>Repeated order confirmation until a marketing campaign is over</td>
</tr>
<tr>
<td>Wrong number</td>
<td>0.9%</td>
<td>A client specified a wrong telephone number in an order; consequently, it is impossible to reach him/her.</td>
<td>Organize order confirmation by e-mail (described above) along with a telephone call by the operator</td>
<td>Sending an e-mail notification for order confirmation.</td>
</tr>
<tr>
<td>A marketing campaign is over</td>
<td>50%</td>
<td>A client ordered when a marketing campaign is over, or it was impossible to reach a client by a telephone while a campaign was running</td>
<td>Organize efficient calling of clients</td>
<td>Notifying the call-center operator about an urgent telephone call to a client</td>
</tr>
</tbody>
</table>
Phase 3

The next phase is the implementation and automation of a business process and, respectively, implementation of control measures of ORM. For that it is necessary to design a business process with the help of subject-oriented modeling (let’s model a function of making a call to clients as an example). Three parties involve in the realization of this function: a call-center, a buyer, an order registration system.

When a new order arrives, it is transferred to the call center, in a positive scenario a call center operator gets in touch on the phone with a client, the client confirms the order, the operator enters the order into a list of confirmed orders and sends this list to a warehouse when a marketing campaign is over. Based on the results of OR analysis, the process was supplemented by alternative scenarios. The process was extended by control measures of OR in the form of additional functional states in accordance to the control measures given in Table 1.

In order to minimize risks of refusal of expensive orders, modeling of business rules in the business object Order has been used: if the order price is more than a defined value, set a high priority to this order (see Figure 1). Business rules are a flexible control measure, since it is easy to add new business rules as long as new risk patterns emerge. They are defined based on working procedures, organizational procedures, instruction of regulatory bodies.

![Figure 1. Modeling of business objects and business rules](image1.png)

The business object is linked to the function “Making calls to clients” and appears in the form of an order during its execution (see Figure 2). As an additional control measure a correctness of the entered product number is checked.

![Figure 2. Business object «Order»](image2.png)
Phase 4

The phase of controlling and monitoring process execution comprises identification, analysis and planning of newly occurred risks, tracing of identified and constantly supervised risks as well as inspection and implementation of response actions and evaluation of their effectiveness. Meanwhile, it is necessary to consider the effectiveness of each control measure within a process, cash equivalent of monetary flows associated with this process and costs of control measures. The fundamental components of internal control of operational risks should include:

- means of internal control – used to protect assets and assure the reliability of financial records. Financial records may include transaction details and intermediary balances. All these information should be reflected in business objects during the process execution.
- means of operational control – used to guarantee a compliance with business goals. These means may include operational plans and budgets in order to compare the real functioning with the planned one.
- means of administrative control – used to guarantee operational effectiveness as well as compliance with politics and procedures established in the company. These means may include internal and external auditing.

Compliance Management is a modern approach to improving organization’s effectiveness through the compliance of control measures that are defined in ORM. A company constantly monitors standards and requirements regarding business and information systems, evaluate risks associated with a mismatch between business and standards and defines priorities for modifying business processes and information systems.

The most adequate way for forming requirements described above is provided by the modern approach to improving the company’s effectiveness called active compliance management. The problem is that information systems as well as processes are not so flexible and easily modifiable due to multiple and often hidden inter-process links. Therefore, an organization’s employee should additionally verify the compliance of obtained results with multiple requirements. The core of active compliance management is means of process self-modification that are inherent in processes themselves. By applying subject-oriented approach control measures could be embedded into a business process execution within a short timeframe. This approach allows to easily modify a process in such a way that it will comply with new requirements. However, in order to achieve this result it is necessary to have a comprehensive understanding of the process, how it is realized by particular performers, i.e. it is essential to know its natural way of execution. The design of such a model is almost impossible using standard modeling tools, since it is necessary to decompose the process to the level of concrete process performers.

3. CONCLUSION

In order to effectively manage operational risks, response actions to unanticipated circumstances should be defined beforehand to ensure a maximum fast recovery from the crisis. The list of measures for reducing (minimizing) an operational risk should include extension of the area of a controlled risk by identifying the maximum possible number of operational risk factors and lowering or eliminating their negative impact on the company’s operation through better business regulation, business process optimization, reallocation of functions, authorities and workload, automation and implementation of information security measures, personnel training, better internal auditing.

In resource planning systems by applying the bottom-up approach operational business process management is realized in a fragmented way, on the level of distinct areas (cost centers), therefore business process reengineering and improvement should be designed as an integrated and holistic process of restructuring individual business processes based on strategic modeling of transformations and ORM. The functions of risk managers are changed in new system models – their core task is to help experts in solving problems that might arise during a process execution. Thereby, managers are able to control risks of business processes and involve new technologies for ensuring security.

REFERENCES