AN ATTEMPT OF SYSTEM APPROACH TO OPERATIONAL RISK MANAGEMENT

A.Gromoff
Science & Education Center of Information Control Technologies, Russia
Email: Alexander.gromoff@me.com

J. Stavenko
BPM chair, Business Informatics department
National Research University HSE, Russia
Email: ystavenko@hse.ru

ABSTRACT

Operational risk management (ORM) is considered as decision-making tool to systematically operational risk identification and determination of the best courses of action for any given situation. Here we made an attempt to analyse ORM from the position of system approach to the enterprise management. In this view, 4 interrelated subsystems were identified: beliefs, constraints, control and monitoring; and ORM is considered as meta-process, which umbellates enterprise business processes and sets requirements to the above subsystems. Interrelations of the management components are discussed as well. The given research was held in a frame 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 open source software (OSS) basis due to increase management efficiency of innovative activity of the enterprises in modern Russia economy».

Key words: Operational Risk, System, Entropy, Knowledge, Risk Management
Paper Type: Research Paper

INTRODUCTION

Traditionally ORM was considered in respect with certain mathematical models application based on collected statistic of failure actions in organization or enterprise. Quite a number of attempts were done to get stable results from the management point of view while implementing “top-down”, “down-top” classic solutions, but in vain. Mainly because of that in many companies the problems of implementation and analysis of integrated risk-management aroused, which are highly dependent on organization and corporate structure and management.

All that came out from an unclear understanding of the place and the role of ORM system in the whole system of company management. This problem was tried to be solved by using the COSO and other standards. Unfortunately, the COSO materials are poorly designed from the practical point of view [2]. Here is ORM considered as a simple six-step process, which identifies operational hazards and offers to take reasonable measures to reduce risk to personnel, equipment and mission. As well a description exists of how a standard process of risk management should be designed but here is no explanation of how the organizational structure should be organized and how the process of risk management should be

implemented. All these have lead to that the companies again had to return to classic fragmentary risk management or to refuse from integration methodology at all.

Organization as an open system

If to consider organization from social-technical system's point of view (technical systems operated by organized groups of people), we can expect that the development of the organization will be provided by the trajectory in a way of state-to-state system transformation under the regulation of many internal and external parameters. These parameters are characterizing the current state of the system and represent the stochastically linked random values from the common view, but actually these values are not that random (the proof of that statement is in consequent article).

The fundamental challenge in managing social-technical system is the need to operate safely under uncertainty and growing risk of failures. As long we manage social-technical system we deal with information in the operations of business processes, and from this point of view all what is done in management has informational nature and risk management should concern informational risks in a stream of the required/send/received/created by business process information.

Operational risk can be considered as an event with certain probability of negative impact, which accrues in business-processes and thereby influences on the willingness (possibility) of the system to achieve the goals and stay in the frames of set trajectory of development. Operational risks are the events that stimulate the appearance of bifurcation points, e.g. deviation from normal trajectory of system movement.

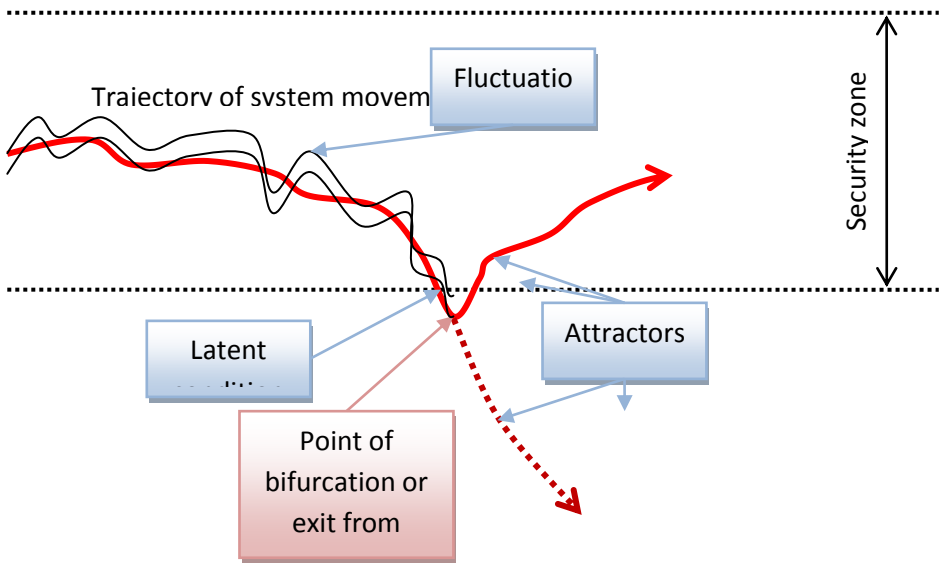
Operational risks can be eliminated both in social and technical subsystems. But recent researches have shown that 99.8% of what previously considered as a result of technogenic risk factor has a social roots, namely, human origin, and since should be considered in a range of operational risks. That is why we consider just operational risks of social origin and in this case the problems of interaction inside complicated management structure, corporate underestimation of possible risks, low effectiveness of compliance management or its ignorance, lack of adequate competence of the employees and their ambitions, all these factors each or in any combinations later or earlier would defiantly lead system to the point of bifurcation.

The realization of operational risk and quantitative estimation of losses will always be the random value that depends on the random parameters in the concrete moment of time. Differ from the standard Brownian movement, the value of these parameters will not increase linearly with the time because social and especially technical subsystems are restricted by the applied control, putting on them (rules, procedures, KPI and so on). This system parameters and controls form the construct which can be named “security buffer belt”.

Marcus and Nichols described an organizational ‘band of safety’ [3]. According to this model, organizations ‘drift’ within an acceptable performance envelope. Warnings of impending danger are signaled by increased rates of minor incidents and accidents. The organization can take action and correct the deviation recognizing, “Correction depends on the magnitude of the signal, the sensitivity of detection and the width of the detection recovery zone” [4]. When the organization is very close to the security border, the amount of insignificant incidents and misadventures has arisen that are the signals of it. Organization can take measures and improve the deviations.

The correction depends on the signal intensity, the sensitivity of problem disclosure and the width of restoration zone. The exit from this "security zone" is equal to the increase the acceptable risk level that is the realization of risk event. Incident can be compared with the release of potential destructive energy if the system, that leads to huge amount of loss, dependent on the size of release. In such case the potential energy can be interpret as an accident, waiting for its time, or the destructive-latent condition, waiting for the trigger (event) for potential release. When the energy is released, the system either returns to the initial condition after corrective action or lose its action. Principally, the destructive-latent condition can be found before the accident has happened.

FIGURE – 1: SYSTEM TRANSITION FROM DESTRUCTIVE-LATENT CONDITION ON NEW TRAJECTORY OF DEVELOPMENT



Thus, to control the exit from the security zone this ability should be implemented into the business-processes, which will resist uncontrolled growth of entropy.

An interdependency of quality, risk, knowledge and information entropy indicators for complicated systems are shown on pic.2. The change of any of the indicators consequently changes value of all others.

FIGURE – 2: THE SCHEME OF QUALITY (Q), RISK (R), KNOWLEDGE (K) INDICATORS AND ENTROPY (E) INTERDEPENDENCY

The relation between management categories, which is shown on the picture 2, has the following characteristic: system appurtenant Knowledge is proportional to the Quality and inversely proportional to the Risk. If Knowledge and Quality are the one shoulder of management lever then the Risk and Entropy are the opposite. Here to continue we need to give the definitions of such every day and qualitative terms as Knowledge, Quality and, of course, Risk and Entropy [5].

Definitions

- Knowledge is the essence of information that is required and materialized while decision capture in system.
- Quality is the adequacy level of a solution required as a reaction on internal or external changes in system. The adequacy is the minimum from the configuration integral by time from the solution square.
- Risk is the price of freedom of making decisions otherwise it is integral by time from the volume of freedom degrees (uncertainty) during the decision-making.
- Entropy is the level of uncertainty during the decision-making or ratio of the decision-making irrelevant information volume to the volume of relevant information. Thus in case of 50/50 we get entropy level equal 1.

Different combinations of the parameters of social and technical subsystems gives the opportunity to form and display the synergetic effects, determining the potential opportunities of choosing different attractors (state of Knowledge, quality, risk and entropy of the system in concrete moment of time), including the different strategies and alternatives of development. For example, during the supply process, the delays of the contract signing and inobservance of contract conditions are the most critical from the correlation between the frequency of risk realization and its consequences point of view, this require the development of preventive actions for decreasing the level of risk criticality. Thus according to the FMEA methodises, during the most effective internal control of the contract preparation process by the legal department, the increase of risk reveal probability and corresponding frequency decrease is awaited [6]. For the security zone determination the VAR method can be used, where for each singled out risk the cost of risk is determined.

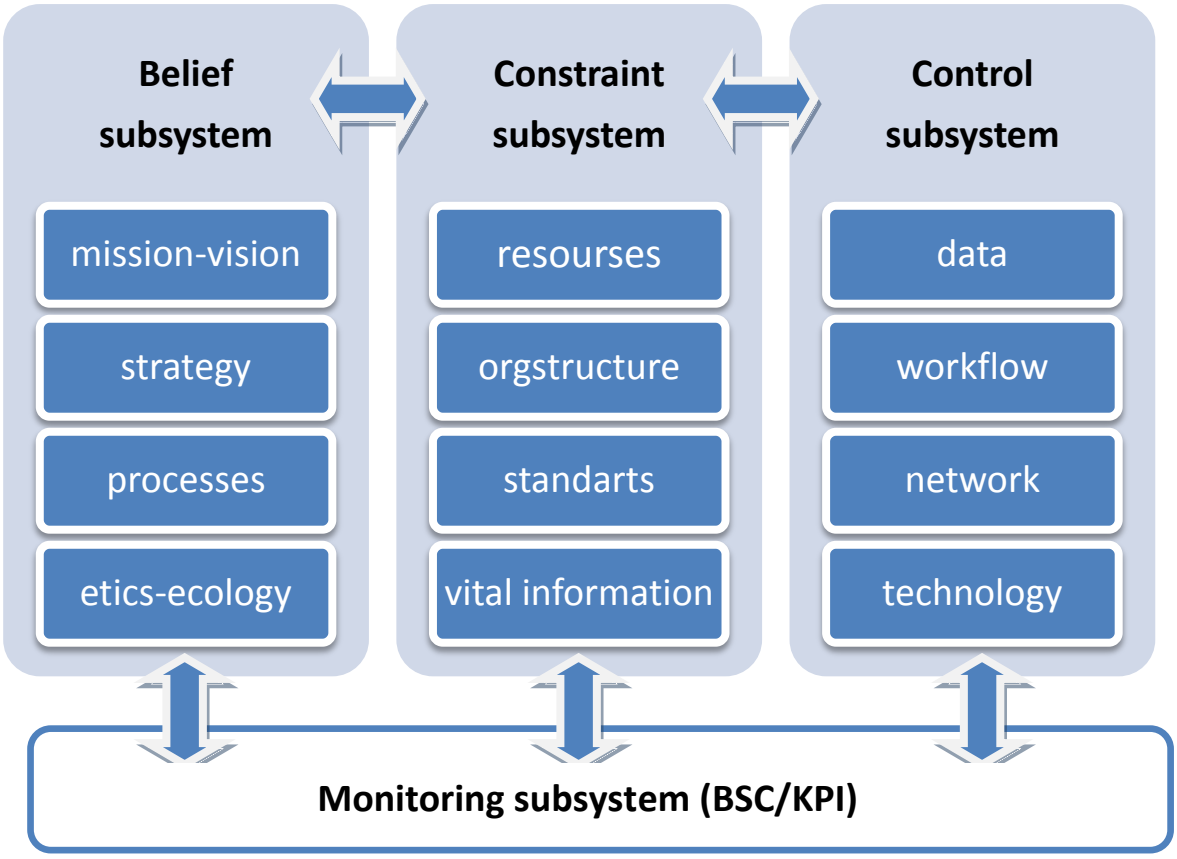
Thereby the operational risk management is an organized, conscious and purposeful activity (the combination of receptions and methods) of influencing on process of system movement through the subsystem parameters changes (parameters of right structure, culture and technical resources) that is the system entropy can be decreased by the means of organizational tools. Based on definition 1,4 it is possible to calculate current value of entropy in particular execution process point, and consequently obtain corresponding values for all process. Further monitoring deviations from obtained figures we get powerful tool for on-line operational risk control and management.

The implementation of operational risk system management

The implementation of complex (holistic) risk management system is possible only if ORM as meta-process runs through both social and technical subsystems of organization. This is achieved by means of the interconnection the following subsystems, which limit the system and form the security belt-zones (picture 3):

- The belief system – a set of documents, spread among the employees, where the basic corporate values, goals and directions of company's development are fixed (declarations about mission, vision, announcement of goals and values). There should be hold a lot of events, which have to be aimed on support of collaboration and loyalty between employees, increasing professionalism and personal effectiveness. Moreover, the number of employees' being informational motivated has to be increased that allows to avoid negative situation, which is initiated by information misinterpretation, demotivated employees and damaged organization's reputation in general.
- Constraint frame – a set of the rules, which regulates acceptability of the certain actions during task/problem solving. This system concludes legislative acts and code of business running, where prohibited actions and behaviour are determined. The goal of the constraint frame is to obtain the frames of security zones and avoid risk of improper action appearance.
- Control system – set rules and procedures, directed on workflow and security management. The goal of the control system: information and assets management and security.
- Monitoring system – set BSC/KPI for monitoring and assessment of the organizational activity. The goal of the monitoring system: the effective implementation of the work.

FIGURE – 3: SUBSYSTEMS IN THE PROCESS OF RISK MANAGEMENT.



Belief system

The corporate policy of corporate values, described in the mission, should be implemented. Mission should represent only formal document, but it should mean routine behaviour of the employees according to the corporate code. Corporate code should involve such values as loyalty (each employee should feel himself as a part of the company), collaboration (general objectives can be achieved only together), patterns of conduct (the success and wellbeing of the company's employee, its clients and partners depends on actions and movements), personal effectiveness and professionalism. The development of competencies should be supported by the system of motivation, system of education and so on. Thereby, the code is the base for creating the corporate culture, based on real, shared, but not declared, values of creating the system of internal communication, determining of common goals and company ideology. In addition the implementation of clear formulated values solves other problems, reducing to a minimum the internal conflicts and also increasing the image of the company for the social environment. For all goals the appetite (the quantitative indicators – borders, determined the maximum acceptable level of risk, which company is ready to accept before the implementation of corrective measures is required) should be set.

Constraint frame

The constraint frame is needed for setting the security zone, including legislative acts and code of business running. First of all the constrain frame should be implemented in transparent and controlled business-processes, since it's designed for ready-to-go processes.In the course of process analysis the following operational risks can be marked out:

TABLE – 1: RISKS IN THE PROCESS OF PROCUREMENT AND SUPPLY

Identified risk	Risk consequence	Frequency (in a year per 100 purchases)	Probability of risk realization	Possible loss in money terms	Risk owner
Violation of submission terms of applications for the resources acquisition	Shift the deadline for the application submission, the Failure of the supply of material resources timing	3	0.05	570, 000 (shifting the deadline on 1 week – 5 working days underproduction on 30% of production in time)	Production department
The error of calculation of the required resources	Purchase in excess of the needs of production => Pointless diversion of funds, the additional costs to the rental place	5	0,01	20,000 (Excising purchase on 10% maintenance of place units for 300 sq. m.) +200,000 (excising purchase on 100% maintenance of place units for 300 000 sq. m)	Production department
The choice of an incompetent employee responsible for the purchase	Failure of the timing of the supply of material resources, the Additional costs	1	0,01	570, 000 + 280, 000 = 850, 000 (shifting the deadline on 1 week – 5 working days underproduction on 30% of production in time and penalties 20% of contract sum)	Procurement manager
The lack of cost analysis of possible supply sources	Acquisition of material resources at inflated prices => The formation of alternative costs	7	0,1	27,000 (Buying products in the price diapason on 10 % higher)	Responsible for purchase

For example, risk “Deficiency of budget for the invoices payment” is one of the most critical risks in the process of procurement, therefore during the business-processes description the behaviour of the employees in case of not only positive outcome (the signing of the contract for procurement, payment request are passed to the accounting department and from there comes the information about payment execution) but also the negative outcome (from the accounting department comes the information that the payment can be executed in several

weeks) should be described. Very often employees do not understand what to do in such situation: negotiate with the supplier, correct the volumes of production and so on. Also in the procedure the answer should be given – how to decrease the probability of such situation (through the budget management, forecasting of cash flows and so on).

Another critical risk of the procurement process is the risk "Non-observance of delivery terms", which may leads to the production disruption. It should be pointed in the procedure – what to do not only in case of receipt of the poor-quality goods, but also in case of receipt of goods at the wrong time.

After risk determination, it is necessary to range them for changing the control measures implementation for risks with high priority. During this, the classical methodises of risk management can be used, such as FMEA (Failure Mode and Effects Analysis). The main idea is the estimation of each risk for several quantitative parameters. At first, such parameters are the risk realization probability and the gravity of its consequences; in some cases the probabilities of risk disclose at the early stage (when it can be properly reacted without significant consequences for process outcome) is also estimated. For every parameter the estimation scale should be determined.

TABLE - 2. THE CONSEQUENCES OF RISK REALIZATION (CRITERIA ARE GIVEN FOR NEGATIVE RISKS)

The consequences of risk realization	Points
The minor. The consequences of the risk are easily eliminated. Total damage does not exceed the sum of the contract for the supply of materials	1-4
Considerable. Implementation of risk leads to downtime/disrupts the process	5-7
The critical ones. Implementation of risk leads to the end of the process. Total damage exceeds the amount of the expected revenue from sales	8-10

TABLE - 3: THE CHARACTERISTIC FREQUENCY OF RISK

The characteristic frequency of risk (in a year per 100 purchase)	Points
Less 2	1-2
3-5	3-4
6-8	5-6
7-9	7-8
10 and more	9-10

TABLE 4. THE PROBABILITY OF DETECTING

Probability of risk detecting	Points
Very likely, the event easily Identified with due control	1-2
High, identification of the events is simple, requires regular compliance audits	3-4
The average, the event may only identify with the application of special methods	5-6
Low, the event is not identified by the special methods of risk management	7-8
Very low, this event it is impossible to identify	9-10

TABLE – 5: THE FMEA ANALYSIS FOR RISK IDENTIFICATION

Identified risk	Possibility to be detected	Probability of risk realization	Severity	Occurence	Detection	reduced no. of risk
Violation of submission terms of applications for the resources acquisition	Yes	0,05	6	3	1	18
The error of calculation of the required resources	Yes	0,01	3	5	2	30
The choice of an incompetent employee responsible for the purchase	Yes	0,01	7	1	5	35
The lack of cost analysis of possible supply sources	Yes	0,1	1	6	2	12

Thus for the risk with the highest priority "Non-observance of the delivery terms" it is necessary to develop the constraint frame at first.

Control system

Companies are also needed with the systems of strict internal control for cash, equipment, and documents. Control and analysis of the procurement process is hold according to the set of goals and tasks of procurement management. Traditionally such analysis involves:

- Analysis of the procurement conditions and of the suppliers market;
- Control of the procurement budget;
- Financial activity analysis;
- Monitoring and analysis of the purchased products quality;
- Monitoring and analysis of procedures for the material resources and finished products delivery;
- Analysis of the system of demand forecasting and etc.

There are two types of control. The goal of internal control – is the defects detection and the adoption of operational measures on their elimination. Internal control is executed after the end of each productive operation that is provided by the technological process. The goal of external control is the compliance with the technological operations, following the regimes of work and other conditions, provided by the technological process, normative-technical documentation and legislative, codes, and professional standards requirements.
Usually the internal operational control is hold with the help of the following mechanisms:

- Double entry, when the entry of the same information from two different – possibly independent-sources (for example, entry the information about the contract into the system by the employee of purchasing department and its confirmation by the accounting department employee);

- The agreement of the results (for example, the agreement of calculation from the purchasing department and calculations from other departments, responsible for the division making support);
- The usage of the warning system (for example, the warning system for worming about the upcoming event – date of contract execution, necessity of running some operations);
- Control for change of the operation condition in the accounting system (for example, in case of changing the contract conditions, it goes through the same agreement procedures as the initial);
- Conducting accounts on operations (for example, error detection in the process of payment) and so on.

The external control – the systems of control procedures from the part of independent departments at the different levels of responsibility and also from the contractors or other organizations. It may be hold by using the following mechanisms:

- Verification of price and other parameters of deals (for example, the verification of the estimation of positions correctness according to the independent external sources data);
- Confirmation of the deals by the contractors (for example, for agreement of deal conditions);
- Monitoring of the activities in accordance with the procedures established by regulatory bodies;
- Audits of compliance of the powers of the officials;
- An internal / external audit (audit information can contain the information about the potential problems both in the organization structure and in the business-processes) and so on.

Security means the prevention of operational risks in the emergency situation, criminal risks and information security (control of access to the premises, screening on admission to work, check of contractors for their connection with criminal structures, protection from unauthorized access, redundancy of information and equipment, etc).

Monitoring system

Determining the effectiveness of procurement operations it is necessary to fully estimate the work of firm's procurement services. The execution of procurement plans on volume and quality indicators, the compliance with budget of the firm, the volume of savings etc. is taken into account. It is possible to approximately determine the cost of one or the other operation in the process of procurement functions executions. Tracking in such manner the whole activity of procurement department, it can be judged about the effectiveness of department, and also can determine the existing problem moments.

There are three main indicators, according to which the control for the procurement department function is occurred: time, price and the suppliers' reliability. Control for the time indicator means the control of delayed delivery and the consequences of such delay. Doing this, such indicators as, for example, the share of detainees orders, the proportion of cases, number of cases of production suspension as a result of the delay, etc. The "price" factor means the price analysis that has been paid during the procurement, particularly their comparison with planned prices and also the attempts to avoid the budget deviation. The suppliers' reliability means the equivalence of quality and volume of the delivery, fixed in the contract, for example, with such parameters as the share of overdue delivery and failure of

the supply; the share of supply, not the relevant treaties concerning the quality of products, etc.

The system approach to the risk management allows to get the whole picture of all operational risks, and not only reveal risks, but also to develop an effective system of actions to minimize the operation risks, including four interconnected systems: monitoring, control, constraint frame and belief system. On the base of developed systems the complex work of regular risk management can be established to reduce the possible losses from risk. All these factors allow passing from the fragment, irregularly "expert" limited risks to the continuous integrated control over the wide variety of risks.

This work was dedicated to the complex vision of operational risk management approach, from administrative forms to automate. It became clear that transferring scope from administrative activities to automatically executed risk controlled procedure we are able seriously decrease probability of system damage and financial loses while instantly increasing risk appetite for acceptable price. Experiments provided in the work frame proved that accuracy of risk determination on a platform of entropy calculation is permanently increased in time of control system run. Thus at the end of the 1-st month of experimental run-off a number of allocated operational risks increased 7 times and continued to crease later, this immediately was reflected in productivity and accuracy, and as a result in companies profit.

High effectiveness of risk management systems is expressed in:

- Flexibility and adaptability, e.g. the willingness to adaptation to the rapidly changing conditions, high speed of response, the ability to quickly cope with adverse situations.
- Adequacy, e.g. the compliance of the implemented risk management procedures with a specific situation, such as the ability promptly to provide all the resources necessary for the achievement of the set goals.
- Effectiveness, e.g. ability to overcome the negative consequences of adverse situations with a minimal amount of resources.

REFERENCES

1) Basel Committee on Banking Supervision. International Convergence of Capital Measurement and Capital Standards (2004). June. — www.bis.org

2) http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf, "Enterprise Risk Management - Integrated Framework", Retrieved March 23, 2011

3) Marcus, A. and Nichols, M. (1996, August). Acquiring and Utilizing Knowledge in Response to Unusual Events in a Hazardous Industry. Paper presented at the Annual Meeting of the Academy of Management, Cincinnati, OH.

4) Marcus, A. and Nichols, M. (1999) On the Edge: Heeding Warnings of Unusual Events. Organization Science, 10 (1), 482-499.

5) Gromoff A., Stavenko Y., "Entropy approach to modeling business processes." Proceedings of the III International Scientific Conference "Prospects of development of information technology." Novosibirsk State University (2011)

6) McDermott, Robin E.; Mikulak, Raymond J.; Beauregard Michael R. The Basics of FMEA. — Productivity Press, 1996.