MODERN MANAGEMENT REVIEW **2020**
MMR, vol. XXV, 27 (1/2020), p. 51-58 **January-March**

Piotr MAKOWSKI[1]

IDENTIFICATION OF COMPONENTS OF OPERATIONAL RISK GENERATED BY INTERNAL FACTORS IN THE COMPANY

The article is devoted to the issues of identifying the components of operational risk in the company, the source of which are the threats caused by internal factors, with attention paid to the possibility of improving the company's internal control system and internal audit in the implementation of the tasks of identifying the risk in question by proposing an additional source of information about adverse events in the form of a system of anonymous individual employee reports. Conclusions from pilot studies carried out among the managerial staff of selected companies were also presented, concerning the conditions necessary to achieve a possible success of implementation of such a system in companies where its functioning is considered necessary.

Keywords: operational risk, audit, internal control.

1. INTRODUCTION

The management of a company usually requires making decisions in conditions of certainty, measurable uncertainty (risk) and uncertainty (in the strict sense – not measurable), whose aim is to achieve the assumed objectives resulting from the adopted strategy and its mission. The assessment of the significance of the impact exerted by a portion of autogenic threats on the achievement of these objectives involves the assessment of an important component of operational risk. The very identification of this risk, which is the task of the company's managerial staff, increases situational awareness, necessary for the implementation of the company management process. Regardless of the applied standards of risk management, each company needs to develop its own methods and tools to identify this risk, which are tailor-made to some extent. It can be assumed that in companies where tasks related to operational risk management are carried out, there exist and are used key risk indicators (KRI) in order to provide early warning about the degree of probability of materialisation of known threats in different areas of company's functioning. They are used to monitor risk factors and the state of protective barriers to prevent increased exposure of the company's potential to threats. Moreover, there are known symptoms which are precursors of unacceptable negative phenomena, so called key performance targets – KPT, which prove the need to implement corrective actions.

[1] Professor Piotr Makowski, PhD, Faculty of Management of Command, War Studies University, 00-910 Warsaw, Al. gen. Antoniego Chruściela „Montera" 103, e-mail: makowski.p.j@gmail.com; ORCID: 0000-0002-3045-3495.

Whereas the development of companies forces the implementation of widely understood changes. They also determine the level of operational risk. Taking into account changes is an important challenge for risk management entities in a company. A necessary condition for effective assessment of operational risk in such situations is to provide current, comprehensive and objective information on the values defined by KRI and KPT allowing to draw conclusions on the level of operational risk, as well as on negative phenomena which, as a result of analyses, must be qualified to these categories.

The aim of this article is to present a proposal of a systemic way of using already known tools supporting management in companies to perform this identification, such as the internal control system and audit in connection with the results of the postulated system of anonymous individual employee reporting. The addressees of these proposals are medium and large companies, where it is possible to use them (in small companies it is difficult to keep the postulate of anonymity of notifications).

2. OPERATIONAL RISK, RISK IDENTIFICATION

"Operational risk is the risk of material and reputational loss and legal liability arising from inadequate or unreliable processes and their necessary resources (personal, material, informational and financial), and arising from disruptions resulting from internal and external threats" (Zawiła-Niedźwiecki, 2013).

Similarly, Michał Thlon (2016) believes that "Operational risk is treated as the possibility of incurring losses due to insufficient or defective systems, incorrect procedures and methods of operation, human errors, technical failures and external events".

These definitions clearly define the internal factors of operational risk, while external events are less precisely defined. E.g. For example, Krzysztof Maderak (2010) includes losses resulting from natural occurrences such as: earthquakes, floods, hurricanes, but also criminal activities such as: terrorism, robbery, theft, vandalism, physical and virtual burglaries. The risk associated with these threats is the so-called "pure risk", which can usually be insured or mitigated by using physical and technical safeguards. The field of interest of this article leaves only that part of the operational risk which is derived from internal factors, and its identification and mitigation is the responsibility of the company. it is worth noting that this part of the operational risk does not have to be solely pure risk. The introduced changes in companies are usually sources of both opportunities and threats, which generates the so-called "speculative risk".

Risk identification is presented as the second stage of risk management in the division of this process proposed by Michał Thlon (2016). It is preceded by the stage of defining objectives. Assuming that defining the organization's objectives is the task of the organization's manager, it can be considered that they should be known to the risk managers. In order to identify risks effectively, it is more important to determine the horizon and context of risk assessment in the first stage of risk management, which takes into account a general example of a risk management scheme according to one of the known risk management standards compliant with the PN-ISO 31000 standard (2018, p.V, fig. 1), according to which risk assessment stages are preceded by determining scope context criteria. In risk assessment, on the other hand, the following stages are distinguished: risk identification, risk analysis and risk evaluation.

The location of risk identification as a stage of risk management shows that its aim is to create conditions for effective implementation of the next stage. As far as pure risk is concerned, this is well reflected by the following statement:

> "The purpose of the risk identification is to compile a complete list of risks resulting from possible events which, depending on the circumstances, may create, prevent, limit, accelerate, delay or hinder achievement of a goal. Risk identification is a continuous activity, because the risk not detected on time or its factors may not only prevent the achievement of a goal, but also pose a threat to the organization" (Abgarowicz et al. 2015).

Similarly, according to Tadeusz T. Kaczmarek (2006) "...risk identification includes the identification of causes and sources of threats and circumstances that may contribute to failure to achieve a goal".

The need to identify both pure and speculative risk is taken into account by the ISO:2018 standard: „The purpose of risk identification is to find, recognize and describe risks that might help or prevent an organization achieving its objectives. Relevant, appropriate and up-to-date information is important in identifying risks" (PN-ISO, 2018).

The definitions quoted reflect the material scope of the risk identification.

Looking at the risk identification from the executive side, it can be concluded that it concerns the collection of information on risk factors and symptoms[2] and, with regard to phenomena previously known for which KRI and KRT were defined, the identification of the intensity of these indicators in the company. In practice, the acquired information refers to widely understood inconsistencies in the procedures for the company-wide implementation of processes or facts (phenomena) that indicate a decrease in the quality of the obtained effects of these processes. Treating the risk identification as a stage of information security of the analysis stage, it needs to be noted that not always the acquired information is sufficient to define quantitative relationships between the causes and the forecasted effects, but it also needs to be pointed out that it allows to increase the situational awareness of decision-makers of a given company.

If a new symptom of a so-called "Top Event" is detected, both its possible causes and its possible consequences must be identified in the long term. A natural tool to organize the search for a solution is the so-called "event trees" and "error trees" or their combination in the so-called "Bow Tie" analysis. On the side of the causes, risk factors (threats), the state of preventive barriers, escalating factors and the state of barriers weakening their influence (so-called Escalation Factor Barriers) are analysed. On the side of the forecasted effects, possible consequences and the application of rational corrective barriers are analysed. The essence of this approach is illustrated in Figure 1. Whenever possible, efforts should be made to attribute specific values of the corresponding probabilities as **components of operational risk** to the individual consequences.

[2] A symptom of risk is to be understood here as observable phenomena, behaviours, of symptoms nature, which are precursors to possible future consequences associated with taking a risk, as opposed to risk indicators showing the intensity of the impact of a given risk factor on its level (KRI).

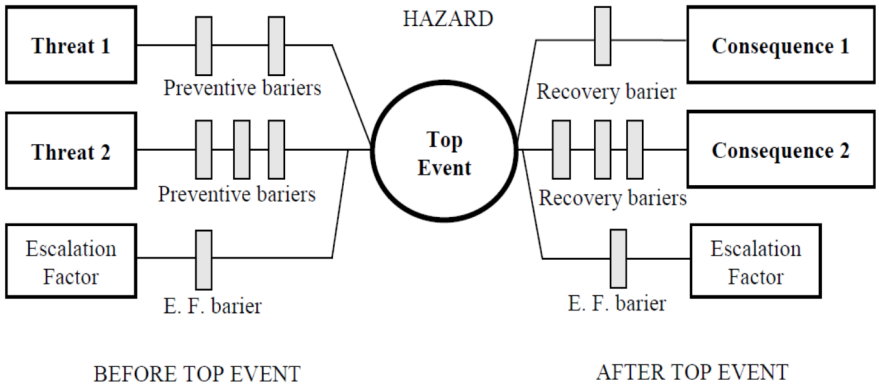

Fig. 1. Illustration of the essence of Bow Tie analysis
Source: Own study based on (Fabbri, Struckl, Wood, 2005).

The Bow Tie diagrams may be subject to necessary updates and additions, including, where possible, the results of identifying the KRI values regarding risk factors (threats) and the KPT intensity that can be attributed to them.

The result of risk identification should be lists of risk factors, and the resulting cause-effect relationships, including KRI and KPT appropriate to the relevant processes taking place in the company and their stages.

3. SOURCES OF INFORMATION IN THE COMPANY ABOUT NEGATIVE PHENOMENA AND POSSIBILITIES OF THEIR USE

When distinguishing within the company: the management subsystem, the executive subsystem and the information subsystem that binds them together, it can be seen that the task of risk identification lies with the latter. In general, the information subsystem is responsible for collecting and distributing information, including meeting the needs of the management subsystem. Information about hazards and symptoms of risk has to be, to some degree, actively sought. It is obtained as a result of the day-to-day supervision of processes in the company by the management and all the entities employed in therein within the framework of their duties, as laid down in the internal regulations. This creates a kind of a system of mandatory reporting on the occurring events, including perceived risks (defined as an internal control system). It should be a sufficient source of information for company management about internal operational risk factors. Practice shows that it also requires periodic control of its operation and improvement, usually in the area of the quality of the performance of internal audit tasks. According to the definition developed by the Institute of Internal Auditors (2016):

> „Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes".

The results of the internal audit may therefore supplement the already existing knowledge of the identified components of the operational risk in the company with new content, thus increasing the situational awareness of the management and leaders.

In tab. 1. a comparison of internal auditing and internal control is presented as viewed by Kazimiera Winiarska (1997).

Table 1. Comparative characteristics of internal auditing and internal control

Term	Internal audit	Internal control
Time criterion	Supervision is effected occassionally and generally later than processes	Day-to-day supervision, continued and parallel in relation to processes
Personnel criterion	The supervising body is independent from the course of economic processes	Supervising body is directly or indirectly dependent from the course of processes
Content-related criterion	Revision is planned and effected through a special instruction	Control is automatically linked to the economic process or effected thorugh special instruction
Organizational criterion	Directions derived from a revision are transferred directly or indirectly to the company's management	Directions derived from a control are transferred to the managers of the supervised processes.

Source: own translation based on (Winiarska, 1997).

The effectiveness of these tools in identifying operational risks can be improved by activating the entire staff of the company. Employee reports are rarely the source of information about negative phenomena. This results, among others, from the fact that informing the management about negative phenomena is often limited in scope and knowledge about them is sometimes held by a limited group, especially in organizations where the principles of fair assessment of the guilt degree ("Just Culture") have not been implemented in practice. This is confirmed by the results of pilot studies conducted using the diagnostic survey method, using the expert interview technique[3]. For example, in certified civil aviation organizations (according to the requirements of EU law) there is an obligation to maintain, in addition to the obligatory one, also an anonymous system of individual employee reports about observed irregularities threatening the safety of air operations. Therefore, in these organizations, the process of functioning of the rules ("Just Culture") has been going on for years and there, the system of anonymous reports, as it results from the research, is a source of a smaller stream of information about negative phenomena in comparison with the system of obligatory reports, but many of these reports are important in identifying new phenomena. Moreover, this system is an information supplement to facilitate the analysis of cause and effect relationships necessary for the

[3] Preliminary research, of a pilot nature, was conducted among the managerial staff and employees of selected civil aviation organizations and companies of the Polska Grupa Zbrojeniowa (PGZ S.A.), in 2017–2019. The subject of the research concerned the determinants of success of anonymous systems and mandatory incident reporting in civil aviation organizations and the needs and possibilities of their implementation in PGZ S.A. and other companies. The research was not funded.

assessment of risk. According to experts from civil aviation organizations, the usefulness of this system is the result of the successive increase in awareness of their staff regarding the validity of these systems. In civil aviation organizations, this system is an effective source of information relevant for identifying safety risks, including operational risks.

In companies not obliged by law to apply these solutions, where the effects of unidentified operational risk are postponed, it is difficult to determine the existence of similar solutions, all the same, as declared by respondents in many PGZ S.A. companies, there is an occasional interface used to submit good employee ideas (in the form of a mailbox).

Information from the postulated system of anonymous individual submissions may increase the effectiveness of supervisory control by the managerial staff and its effectiveness in identifying phenomena important for specifying factors and symptoms of operational risk. Moreover, this information should also be taken into account when planning the scope of internal audits. Focusing auditors on verifying information on previously identified negative phenomena has the potential to increase the effectiveness of this tool in implementing the tasks related to the identification of internal operational risk factors, and to check the effectiveness of corrective actions taken previously.

4. SELECTED CONDITIONS FOR IMPLEMENTATION OF THE ANONYMOUS EMPLOYEE REPORTING SYSTEM

According to the opinion of the respondents, who are members of the management boards of the companies, management representatives and employees, the implementation of the anonymous individual reporting system in the companies is be preceded by the implementation of "Just Culture" rules within the organizational culture, if such rules have not been implemented. These principles should be clearly defined, made public and tested in practice in a given company. This is a long-term process. The company postulates to organize a system of individual, anonymous employee reporting. Its functioning should be sanctioned in the company documents. This system should consist of an interface for the reporting entities, ensuring a high level of security of maintaining anonymity and a subsystem for analysing such reports. A proposal to respond to a report after acceptance and approval by the authorised managerial entity should be implemented.

In order to further dissemble the intentions of the entity reporting the incident, the respondents proposed to integrate the interface of this system with complaints and objections systems, good employee ideas etc. Information – reports concerning: threats, irregularities, dangerous events, which, after verification and analysis in e.g. the team dealing with risk management issues and after acceptance of the results of this analysis by the management, should be qualified as information archived in the company's database e.g. as risk indicators, KRI, in connection with risk factors or as symptoms of risk. Such a type of risk, being a component of operational risk identified in the context of its causes and symptoms, would facilitate its further monitoring within internal control and internal auditing. And linking it to a process or an organizational unit would constitute an element of the "operational risk map of the company".

The involvement of employees is a necessary prerequisite for the effectiveness of the proposed system. Among the factors that give hope of increasing this involvement were those that ensure the satisfaction of the reporting entities:

- the speed and accuracy of the response to a report in line with “Just Culture” principles;
- ensuring free access for all workers to information about the content of a relevant report assessed as useful for identifying risks and information about preventive or corrective actions taken, treated as information about the disclosure clause: “for official use”;
- promoting awareness of the risk management methodology adopted among management and employees;
- development of observational worksheets for employees on previously identified disorderly phenomena;
- introduction of the principle of periodical rewarding of employees within organizational units with the best results in risk management, as opinioned by the management.

The second prerequisite is to appoint a competent interdisciplinary team of analysts, capable of selecting applications in terms of their usefulness in risk management, verifying the truthfulness of applications, and above all, using the most important of them to identify specific components of operational risk.

The respondents also expressed concerns about misguided use of the system of anonymous reports, e.g. for personal attacks. On the other hand, such events are signs of deterioration in the quality of human relations and their intensity may indicate the value of KPT in this component of operational risk.

The results of the analysis should be archived in the company's database for a limited period of time determined through evaluating their usefulness.

5. CONCLUSION

Based on the success of the proposed system of anonymous, individual employee reporting within civil aviation organizations, as an important tool in identifying risks to the safety of air operations, it can be concluded that similar solutions in other, medium and large companies should also yield successful results. The implementation postulates identified in the preliminary research are of general nature, in a way mitigating the process of implementation of the system in question and allowing to make the organizational cultures of companies without experience in using the system in question similar to the organizational cultures of civil aviation organizations. These postulates could be the basis for the formulation of problems and hypotheses within the framework of research relevant to this issue in relation to specific companies. If the above was effected, it would be a source of satisfaction for the author.

REFERENCES

Abgarowicz, G. et. al. (2015), *Zarządzanie ryzykiem. Przegląd wybranych metodyk*, ed. D. Wróblewski. Józefów: Wydawnictwo CNBOP-PIB.

Fabbri, L., Struckl, M., Wood, M. (2005). Guidance on the Preparation of a Safety Report to Meet the Requirements of Directive 96/82/EC as Amended by Directive 2003/105/EC (Seveso II), European Communities.

Kaczmarek, T.T. (2006), *Zarządzanie ryzykiem. Ujęcie interdyscyplinarne.* Warszawa: Difin.

Maderak, K. (2010), *Ewolucja metod kwantyfikacji ryzyka. „Miesięcznik Finansowy Bank”*.

PN-ISO 31000:2018-08. Zarządzanie ryzykiem – wytyczne. Warszawa: PKN.

THE INSTITUTE OF INTERNAL AUDITORS (2016) [Access: 20.02.2018]. Access on the internet: https://www.iia.org.pl/sites/default/files/definicja_kodeks_standardy_pl_en_2017_final_0.pdf.

Thlon, M. (2016), *Podstawy zarządzania ryzykiem operacyjnym.* Kraków: Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie.

Winiarska, K. (1997). Kontrola finansowo-księgowa a auditing wewnętrzny. ZT No. 40. Warsaw: SKwP.

Zawiła-Niedźwiecki, J. (2013). *Zarządzanie ryzykiem operacyjnym w zapewnianiu ciągłości działania organizacji.* Kraków–Warszawa: Edu-Libri.

DOI: 10.7862/rz.2020.mmr.6

The text was submitted to the editorial office: March 2020.
The text was accepted for publication: March 2020.