ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 688 FINANSE, RYNKI FINANSOWE, UBEZPIECZENIA NR 49 2011

ELŻBIETA IZABELA SZCZEPANKIEWICZ
Department of Accounting
Poznań University of Economics

SELECTED ISSUES IN EFFECTIVE IMPLEMENTATION OF THE INTEGRATED RISK MANAGEMENT SYSTEM IN AN ORGANIZATION

1. Introduction

Business risk in an organization increases when the internal control system is not working properly. The great importance of internal control in the effective management of an organization has been recognized for decades. However, only for a few years internal control in organizations has been looked at through the prism of the risk which accompanies their operations. In recent years, various methods and methodologies of identifying risk factors, assessing risk effects and risk management have been developed, both through research and practice.

To a degree, business risk can be identified and measured. An accurate identification of the nature and scope of the possible risk allows taking appropriate measures to reduce it at the right time. Therefore, risk should be identified in all the areas of an organization's operations, in every process and system, on an ongoing basis. However, as has been evident from practical experience, risk cannot be fully eliminated from business operations. Attempts can only be made to reduce it to a tolerable minimum. In order to ensure that the risk management process is effective, it should be tied with the process of designing appropriate control procedures and actions, i.e. with the internal control system. The internal control system procedures and mechanisms, established on the basis of the risk analysis, help to protect an organization against adverse events and to minimize losses, should a given risk occur. The integration of the risk management process with the internal control system should improve the effectiveness of organization management.

The purpose of the present paper is to present the American *Enterprise Risk Management (ERM)* system, published in the COSO II Report. The *ERM* model defines the method of integrating risk management with the internal control system in an organization. The paper discusses the components of the integrated ERM system structure. It specifies the conditions for an effective implementation of such a system. It also points out the most common mistakes made in organizations which have implemented such a system, on the basis of a study conducted in public finance sector entities.

2. The essence of risk management in an organization

Risk management is most often defined as a continuous decision-making process which aids the achievement of a predefined economic or social objective at an optimal cost and with the use of the procedures which help to fully eliminate the risk which may prevent the achievement of such an objective, or to reduce it to an acceptable level[1]. Risk manage-

[1] *M. Zdanowski, Zarządzanie ryzykiem. Próba opisania procedur i określenia obszarów działalności badawczej. Zarządzanie ryzykiem Nr 1, Wyższa Szkoła Ubezpieczeń i Bankowości, Warszawa 2000, p. 9.*

ment is a regular examination of the problem of risk in the entire organization, i.e. the impact of external and random factors and other hazards generated by the organization itself, and the assessment of risk levels, as a probability of the occurrence of particular risks, as well as the implementation of a comprehensive strategy of risk response[2]. The components of the risk management process include**: identification of the organization's objectives, risk analysis and assessment, risk response and risk monitoring.**

Risk analysis and assessment is the basic component of risk management in an organization. This element has to be related to predetermined strategic and operational objectives. The risk analysis process yields information necessary to make decisions concerning risk handling strategies. Organizations use various methods of handling the identified risk. The management of an organization may:

1) **reduce the risk,** i.e. prevent it by taking appropriate control actions and protective measures, this way the risk is reduced to an acceptable level or its effects are minimized, should the risk occur,
2) **transfer the risk,** i.e. use legal methods to transfer the risk onto different entities through risk financing, insurance, hiring the services of specialized third-party companies, etc.
3) **accept the risk**, i.e. tolerate the effects of risk if they are negligible compared to the expected benefits,
4) **avoid the risk,** i.e., for example, discontinue the action which exposes the organization to risk or refuse to take actions associated with high-level risk and the results of its occurrence, or to reorganize the processes in danger and choose the appropriate risk handling method.

Risk analysis is aimed at optimizing (minimizing) the losses associated with business risk. In the risk analysis process the information necessary to make decisions pertaining to the effective choice of risk reducing measures and the assessment of validity of risk transfer, acceptance or avoidance is generated. The managerial information developed in the course of risk analysis also indicates the priorities for the development of the security and control systems, while the assessment of the risk level is a starting point for making conscious decisions regarding the acceptance of a particular risk level with reference to a particular resource (investment, undertaking), as well as for selecting and implementing the appropriate security measures within the security policy developed for a given resource. The risk assessment stage includes risk appraisal and appraisal of the costs of introducing reduction measures for that risk, including control procedures and security measures. The choice of the appropriate security and control procedures calls for the analysis of:

1) the level of the identified risk,
2) availability of security measures, e.g. on the market,
3) the costs of control and security measures,
4) management's security policy (i.e. IT security policy),
5) customary practice in the sector.

[2] *It should be emphasized that risk management is more than a sequence of actions aimed at reducing the impact of adverse factors on the organization, i.e. crisis prevention, but also seizing the occurring opportunities, taking into account the risk costs. Read more in J. Bizon-Górecka, Inżynieria niezawodności i ryzyka w zarządzaniu przedsiębiorstwem, Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego Sp. z o.o., Bydgoszcz 2001, p.12.*

If there is an internal audit system in an organization, an internal auditor assesses whether a selected risk management method covers all the aspects, whether it is sufficient for the type of business run and how clear it is for the key groups or particular employees involved in the organization management process. Should there be no audit unit, the management of an organization is responsible for control.

3. The essence and the structure of the ERM system, according to the COSO II Report

In recent years, many well-know risk management methods have been developed, both through company research and practice, i.e. Enterprise Risk Management (ERM), Value at Risk (VaR), Risk Metrics, SFOC Risk Assessment Scorecard, Simplified Process for Risk Identification (SPRINT), Information Risk Analysis Methodologies (IRAM). The present author believes that the ERM model (announced by the Committee of Sponsoring Organizations of the Treadeway Commission) is a particularly important achievement in terms of risk analysis methodology and management. The ERM model was published in 2004 in the **COSO II Report:** Enterprise Risk Management – Integrated Framework. The Report develops the first version of COSO: Internal Control – Integrated Framework published in 1992. The concepts of COSO and COSO II became global standards.

Today, many institutions and companies worldwide use the concept developed in the COSO and COSO II Reports in the process of monitoring the effectiveness of the risk management and the internal control system. The said standards are also implemented by some Polish companies quoted on the stock exchange and public finance sector entities. On the bases of the COSO and COSO II Reports, the Ministry of Finance developed the management control standards, which the public finance sector entities have been obliged to implement since 2010.

This ERM expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management. While it is not intended to and does not replace the internal control framework, but rather incorporates the internal control framework within it, companies may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a fuller risk management process.[3] The COSO II Report presents a risk management process based on three important notions: business risk, internal control system and creating values in an organization. The COSO II report[4] defines ERM as a process initiated and exercised by the supervisory board, management board, the executive and other staff members to ensure that building the organization's strategy:

- all operations are effective and efficient,
- financial reporting is reliable,
- regulations and internal rules are followed.

The COSO II presents a system composed of eight integrated **risk components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information & communication and monitoring.** The components of

[3] *Enterprise Risk Management - Integrated Framework, Executive Summary, Committee of Sponsoring Organizations of the Treadway Commission, USA, September 2004, p. 5.*

[4] *The COSO Report: Internal Control – Integrated Framework, Committee of Sponsoring Organizations of the Treadeway Commision, USA 1992 and Enterprise Risk Management, op.cit, www.sox-online.com/coso_cobit.html.*

the integrated risk management system operate on four planes associated with the business objectives, i.e. on the strategic, operational, financial and conformity-with-the-law planes, which at the same time are the most important risk management objectives in the organization's operations. According to the COSO II concept, this system should unite the four organization levels, from the operational level, through the strategic level, to the corporate supervision level.

Figure 1 presents the COSO II model.

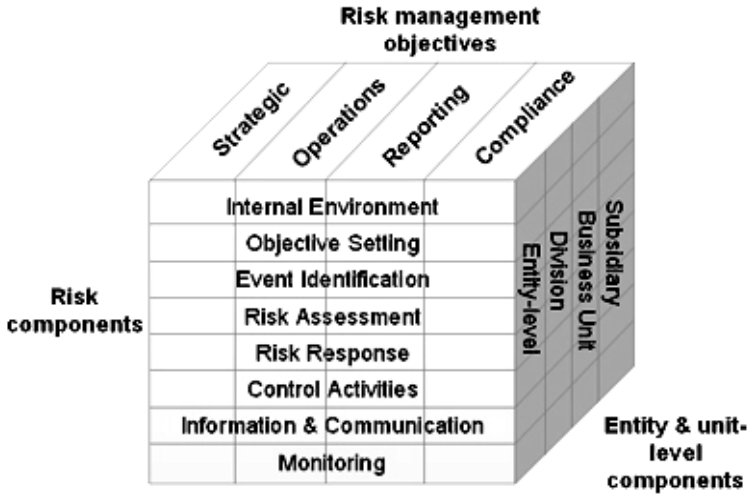
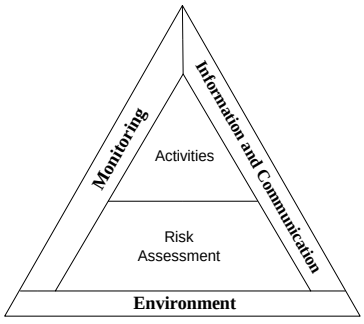


Figure 1. *The model developed in the COSO II Report*

Source: http://www.grc-resource.com/wp-content/uploads/2008/03/coso_erm_framework.jpg.

It should also be emphasized that 5 out of the 8 elements named above form the internal control system structure within ERM: internal environment, risk assessment, control activities, information & communication and monitoring (figure 2).



Components	Funktions
Internal environment	Provides an atmosphere in which people conduct their activities and carry out their control responsibilities. It serves as the foundation for the other components.
Risk assessment	Management must assess risks to the achievement of specified objectives.
Control activities	Are implemented to help ensure that management directives to address the risks are carried out.
Information & communication	Relevant information is captured and communicated throughout the organization.
Monitoring	The entire process is monitored and modified as conditions warrant.

Figure 2. *The model of the internal control system*

Source: own work on the basis of the COSO Report (1992) www.coso.org.

Table 1 presents in detail the components of the ERM based on the internal control system, in particular areas.

Table 1. *Elements of the ERM structure*

Area of control	Elements of the ERM structure	Functions
Internal environment	- Respecting ethical values, - professional competence, - organizational structure, - delegation of authority.	It should provide a general framework for the other elements of the ERM. Elements of the control environment include: values and ethical standards, staff competence features, as well as division of responsibilities and powers resulting from the organizational structure. The unit's executive should ensure correct operation of the of the internal control system and provide all staff members with an appropriate environment for the understanding and proper performance of control tasks.
Objective setting	- The Mission, - establishing objectives and tasks, - monitoring and evaluating their achievement and completion.	The undertaking should define a set of goals before the executive staff go on to identify risks which may potentially affect goal achievement. Thanks to risk management, the executive staff have goal-setting procedures which refer to the company's mission and vision, and are consistent with the level of risk allowed by the undertaking.
Event identification	- Identification of internal risk factors, - identification of external risk factors, - identification of market chances.	Internal and external risk factors which have an impact on goal achievement must be identified and divided into threats and opportunities. Threats and opportunities are then taken into account in the process of setting goals and building the undertaking's strategy.
Risk assessment	- Risk analysis, - Risk assessment.	Risks are analyzed, considering likeli-hood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
Risk response	- risk response - - remedial measures.	The executive staff are able to select a proper type of risk reaction, i.e. avoidance, acceptance, reduction or sharing – developing a set of actions to align risks with the entity's risk tolerances and risk appetite. At a later stage a set of measures are developed to link different risk types to their acceptable level.
Control mechanisms	- Documenting the control system and supervision, - documenting and recording financial and economic operations, - detailed control mechanisms for operations, - allocation of responsibilities, verification, supervision, authorization, - uninterrupted operations, - protection of resources, - IT system control mechanisms: access control, con-	Control measures should be adjusted to specific risks to minimize the likelihood of risk occurrence or reduce financial consequences of its occurrence. Control measures are a set of provisions and control procedures which are in place to reasonably ensure that the unit's goals are achieved. They comprise: orders; regulations; instructions; procedures; divisions of powers, duties and responsibilities; and the organizational structure. They should be developed for and implemented in all areas in which there are identified risks jeopardizing the achievement of goals. Their aim is to ensure that all activities and measures are implemented in an effective manner. Efficient

	trol of system software, applications, creating changes in applications, allocation of duties, continuity of operations.	operation of the internal control system is determined by free information flow and appropriate communication process.
Information and communication	- Current information, - internal communication, - external communication.	Information and communications system is a system of data exchange used within the unit and between the unit and its external environment. The information flow system operates throughout the entire organization.
Monitoring and evaluation	- ERM system monitoring - self-assessment of the control system, - evaluation through internal audits, - obtaining confirmation of the condition of management control	Monitoring is a process aimed at verifying whether the remaining element function properly. Monitoring of the effectiveness of the internal control system is effected by ongoing review of operations or periodical assessment. Ongoing monitoring is the responsibility of the executive staff in the assigned area of responsibility for particular processes or operations. Periodical assessment is the duty of the internal auditor. Whenever necessary, the internal control system should be modified. In this way, the CS can respond dynamically to changing circumstances or new regulations.

Source: own work on the basis of the COSO Report (2004), www.coso.org.

4. Practical aspects of ensuring the effectiveness of the ERM system

In order to design an effective integrated ERM system, the current situation in the organization, its strategies and operational objectives, the adequacy of the organizational structure, and the allocation of powers and responsibilities have to be analyzed in detail. The management have to determine "the appetite for risk" for each objective, process or action. Before implementing the ERM, the management should assess the already existing mechanisms for risk reduction, identify the hot spots in the organizations and the risk factors which determine the achievement of the predefined objectives. They also need to assess the probability and the effects of the occurrence of the risk (events). They should develop the methods of responding to the risk at an unacceptable level, and in particular the control policies and procedures, as well as the mode of the ongoing and periodic ERM monitoring. For the internal control procedures and mechanisms to be effective, the managerial staff and the employees need to participate in training courses dedicated to the implemented solutions, and subsequently, all the ERM system components have to be monitored. The implementation of ERM should create an added value in the organization. Therefore, the present author believes that the costs-benefit relation should be examined both in the risk management process and in developing the internal control mechanisms and procedures. Depending on the scale and complexity of the organization's operations, the risk management process may be: formal or informal, objectively measurable and subjective, built into a give organizational unit or centrally controlled at the strategic level of the organization.

The process of ERM implementation should correspond to the organizational culture, the manner of management and the mission and objectives of the organization. The ERM process can be recognized as adequate, if it meets the five basic criteria:

1) the types of risk resulting from the operational strategy and the type of business have been identified and prioritized,
2) the acceptable risk level has been established in all the risk areas,
3) the internal control mechanisms and procedures aimed at reducing the risk to an acceptable level (or any other methods of risk handling) have been planned and introduced,
4) monitoring is used for the purpose of periodic verification and assessment of the risk and the effectiveness of the risk management control tools,
5) the management of the organization receives periodic reports on the risk management process and the functioning of the internal control system.

The present author believes that the eight components of the integrated ERM should be implemented in an organization in stages, in the order specified in figure 3.

Therefore, an integrated management of the risk and the internal control calls for comprehensive knowledge and understanding of the organization's operations.

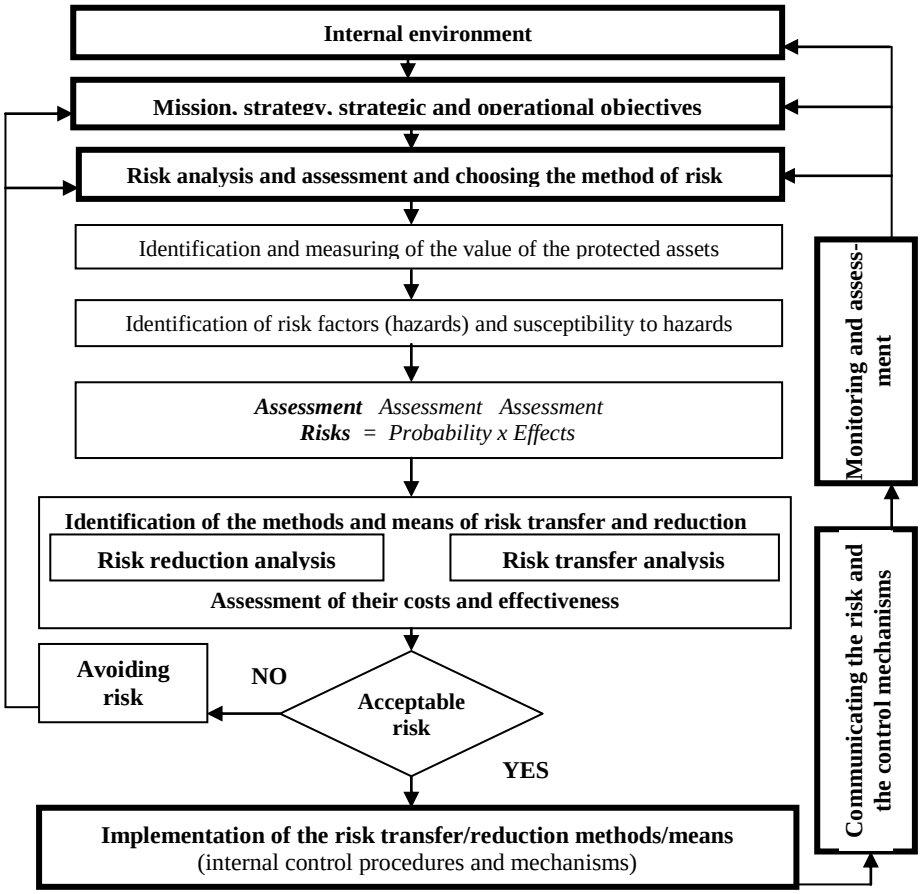


Figure 3. *The process of implementing an integrated ERM system in an organization*

Source: own work on the basis of: E. I. Szczepankiewicz, P. Szczepankiewicz, Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyj-

nym, Część 3 – Strategie postępowania z ryzykiem operacyjnym, Monitor Rachunkowości i Finansów 2006, No. 8.

It is the responsibility of top level managerial staff to develop the ERM, implement it in an effective way and control its effectiveness. The integrated risk management should lead to a better understanding of the particular types of business risk, and as a consequence – to avoiding financial loss. It increases the effectiveness of implementing operational strategies and achieving operational objectives. It may contribute to a more economical and effective use of resources, proper securing of the property, reducing the changeability of income, increasing return on equity and optimizing its allocation. It helps to ensure that the financial and operational information obtained is reliable and that the laws and internal regulations are obeyed.

Table 3 presents the most common mistakes in implementing and operating the ERM system in organizations, on the basis of irregularities identified in public finance sector entities during an internal audit.

Table 3. *The most common mistakes in implementing and operating the ERM system in organizations*

Components	Inadequacies in the functioning of ERM system
Internal environment	- Professional competence of entity employees is not shaped properly - The majority of entities lack a unit or a person responsible for risk management supervision. Sensitive tasks, risk factors and irregularities are not identified, the management are not taking any actions aimed at establishing appropriate remedial measures reducing the occurrence of adverse factors.
Objective setting	- No risk management documentation. - No decision on the acceptable risk level. - Risk management has not been included in job profiles and employee assessment criteria.
Event identification	- No risk registers.
Risk assessment	- No risk assessment (risk probability, risk effects, assessment of their costs and effectiveness).
Risk response	- No remedial action. - No self-assessment of remedial action.
Control activities	- The control procedures are not based on the laws and regulations. - Accounting principles used in the entity have not been established properly: - no documentation specifying the adopted accounting principles, - accounting principles are established and updated by unauthorized persons, - accounting principles are not updated upon the amendment of the laws and regulations in force, - no description of the IT accounting data processing system and the financial data protection principles.
Information communication	- No training programs on risk management and IT polices.
Monitoring	- No self-assessment of internal control system and of risk management.

Source: own work on the basis of: Sprawozdanie - Audyt wewnętrzny i kontrola finansowa w 2006 r., Ministerstwo Finansów, Warszawa, lipiec 2007 r., p. 18-21.

5. Conclusion

In the opinion of the present author, the ERM concept (COSO II Report) presents the most comprehensive approach to the issues of risk management integrated with the internal control system of all the most popular risk management concepts. It can be said that in this concept, the three pillars of risk management are: regular identification of risk factors, analysis and assessment of the risk associated with the organization's operations, and developing and implementing the proper risk manage-ment strategy and internal control system in an organization. In order for risk management to be effective, full integration with all the management processes, and in particular the strategy, operational objectives and the internal control system, is a must. The implementation of an integrated ERM should lead to a better use of the management's skills and abilities, which may result in an effective reduction of the number of emergency situations and the uncertainty of actions, and increasing the ability to achieve the organization's predetermined strategic and operational objectives. It allows a better use of market opportunities and helps to build up the trust of shareholders thanks to the improved corporate governance processes.

6. Literature

[1] Bizon-Górecka J., *Inżynieria niezawodności i ryzyka w zarządzaniu przedsiębiorstwem*, Oficyna Wydawnicza Ośrodka Postępu Organizacyjnego Sp. z o.o., Bydgoszcz 2001.
[2] *Enterprise Risk Management – Integrated Framework*, Committee of Sponsoring Organizations of the Treadeway Commission, USA 2004, www.coso.org**.**
[3] http://www.grc-resource.com/wp-content/uploads/2008/03/coso_erm_framework.jpg.
[4] *Internal Control – Integrated Framework*, Committee of Sponsoring Organizations of the Treadeway Commission, USA 1992, www.coso.org.
[5] Szczepankiewicz E.I, Szczepankiewicz P., Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym, Część 3 – Strategie postępowania z ryzykiem operacyjnym, Monitor Rachunkowości i Finansów 2006, nr 8.
[6] Sprawozdanie - Audyt wewnętrzny i kontrola finansowa w 2006 r., Ministerstwo Finansów, Warszawa, lipiec 2007 r.
[7] Zdanowski M., *Zarządzanie ryzykiem. Próba opisania procedur i określenia obszarów działalności badawczej. Zarządzanie ryzykiem Nr 1,* Wyższa Szkoła Ubezpieczeń i Bankowości, Warszawa 2000.
[8] Dr E.I.Szczepankiewicz, Katedra Rachunkowości, Uniwersytet Ekonomiczny, Poznań.

Summary

The article presents the concept of ERM and the possibilities of its practical implementation for the purpose of managing the risk related to business operations of an enterprise. A great number of organizations worldwide exploit the concept of internal control as presented in ERM in the process of monitoring the effectiveness of risk management and the internal control system. The ERM model defines the method of integrating risk management with the internal control system in an organization. The paper discusses the components of the integrated ERM system structure. It specifies the conditions for

an effective implementation of such a system. It also points out the most common mistakes made in organizations which have implemented such a system, on the basis of a study conducted in public finance sector entities.

WYBRANE PROBLEMY EFEKTYWNEGO WDROŻENIA ZINTEGROWANEGO SYSTEMU ZARZĄDZANIA RYZYKIEM W ORGANIZACJI

Streszczenie

Artykuł prezentuje koncepcję Enterprise Risk Management (ERM) i możliwość implementowania jej do praktycznego zarządzania ryzykiem w działalności przedsiębiorstw. Koncepcja ERM jest coraz częściej wykorzystywana w procesie monitorowania efektywności zarządzania ryzykiem i systemu kontroli wewnętrznej przez wiele organizacji na całym świecie. Model ERM określa sposób integracji zarządzania ryzykiem w organizacji z systemem kontroli wewnętrznej. W opracowaniu omówiono elementy struktury systemu ERM oraz określono warunki skutecznego wdrożenia takiego systemu w organizacji. Wskazano również najczęściej popełniane błędy w organizacjach, które taki system wdrożyły na przykładzie badań przeprowadzonych w jednostkach sektora finansów publicznych.

ELŻBIETA IZABELA SZCZEPANKIEWICZ
Poznań University of Economics