

ФУНКЦІЇ ВНУТРІШНЬОГО АУДИТУ З ОЦІНКИ УПРАВЛІННЯ РИЗИКАМИ НА ПІДПРИЄМСТВІ

У статті розглянуто функції та значення ризик-орієнтованого внутрішнього аудиту в процесі оцінювання ризиків суб'єкта господарювання. Обґрунтовано методи оцінки властивого ризику та залишкового ризику за результатами управління, а також складання звіту за результатами ризик-орієнтованого внутрішнього аудиту.

Ключові слова: внутрішній аудит, управління ризиками, внутрішній контроль, аудиторський звіт

Dorosh N., A. Shapoval A.

INTERNAL AUDIT FUNCTIONS ON ASSESSMENT OF ENTERPRISE RISK MANAGEMENT

The functions and significance of the risk-based internal audit during the enterprise risk assessment are considered in this article. The methods of inherent and residual risk assessment under the results of management and also making a report under the risk-based internal audit are grounded.

Keywords: internal audit, risk management, internal control, audit report

1. Introduction

The development of the audit concept involves the application of a risk-based approach nowadays. It is objectively caused by the necessity for improvement of audit efficiency. The need of a risk-based audit is also increased by the requirements of Sarbanes-Oxley Act, passed in the U.S. in response to the well-known scandals involving Enron, WorldCom, Parmalat. Risk-based internal audit is the most progressive approach to evaluation of the effectiveness of the entity and its internal control system, focusing on the most risky areas of activity. The problem of developing appropriate methods of risk-based internal audit based on positive international experience is particularly relevant to domestic enterprises that face a large amount of risks while accomplishing its objectives.

The problem of development of methodology of risk-based internal audit is investigated in the works of such foreign experts, as P. Griffiths, J. Griffiths, R. Moeller, V. Benes, K. Pickett, Spencer. Among local scientists an attention should be paid to the scientific works of O. Petryk, O. Redko, T. Kamenska, M. Shuhman, T. Bulat, R. Kulik, N. Shalimova.

However, the concept of risk-based internal audit is rather new to Ukraine and requires further investigation and implementation to the practical activities.

2. The concept of risk-based audit

The concept of risk-based audit began to develop in the early 90-ies of XX century and was confirmed in numerous legal and regulatory documents. The need for assessing the risks by managers is emphasized by international auditing standards, particularly by ISA 315 "Identification and Assessment of Risks of Material Misstatement through Understanding the Entity and its Environment" [11]. In 1992, the Committee of

Sponsoring Organizations of the Treadway Commission (COSO) of the United States developed an integrated framework of internal control, one of the basic elements of which was risk assessment as a function of the internal control system. Further development of risk-based approach is associated with the development of the concept COSO ERM (COSO II) «Enterprise Risk Management: Integrated Framework». This concept has complemented COSO, identifying eight risk components: internal environment, objective setting, event identification, risk assessment, risk response, control procedures, information and communication, monitoring. IT-oriented concept of internal control, commonly known as CobiT, among others defines the importance of risk management during the process of IT governance. In 2002 the Sarbanes-Oxley Act was approved, and Section 404 of it had stressed the necessity of risk assessment and defined the managers' responsibility for this process. In May 2013 an updated model of COSO was published. It was supplemented by section "Illustrative Tools for Assessing Effectiveness of a System of Internal Control" [12]. These trends have necessitated the formation of the concept of risk-based internal audit.

The main target of internal audit is to assist the organization in achieving its objectives. From the point of risk-based approach to internal audit, it provides an objective and independent opinion on the efficiency of management of risks by internal control system and reducing their impact on the operations and accounting system.

For internal audit to be successfully held it is necessary to fulfill the following requirements: the company has a system of risk identifying and risk assessment; the Board of Directors determines the risk appetite in terms of risk assessment system; managers

identify and assess risks on a regular basis; the risks are described by the risk register, which serves as the basis for developing the program of internal auditing. Risk appetite is the amount of risk, on a broad level, that an enterprise and its individual managers are willing to accept in their pursuit of value [13, c.125].

3. The objectives “tree” of the enterprise for identify risks

In order to adequately identify and assess the risks it is necessary to define the objectives tree because each risk in any way is related with the specific objectives of the enterprise. Building the hierarchy of objectives allows assessing adequately all risks in terms of their materiality and probability. In international practice, a 5-level approach is established for assessing the risks significance as the multiplication of consequence and probability of risk that has the form of matrix (Tab. 1) [8, c.12]:

risk (RR), which characterizes the level of consequence and likelihood of risk after the implementation of internal control procedures. Then control risk (CR) can be determined in such way:

$$CR = IR - RR.$$

Thus, the objective of the internal control system is to minimize the risk to an acceptable level, and the task of internal audit is to assess the effectiveness of internal controls, that should minimize the risk to an acceptable level (risk appetite). After the identification and risk assessment it is necessary to make a risk register, in which is specified the list of objectives and risks that affect the achievement of those, characteristics of the level of risk impact, source of information about risk (often a special seminar or meeting), and assessment of the consequence, likelihood and significance of inherent risk. Development of risk register is the responsibility of management and it is essential for the further conduct of internal audit. If there is no

Risk Significance Assessing Matrix

Table 1

Likelihood of risk	Almost certain (5)	5	10	15	20	25
	Likely (4)	4	8	12	16	20
	Possible (3)	3	6	9	12	15
	Low (2)	2	4	6	8	10
	Very low (1)	1	2	3	4	5
	Insignificant (1)	Minor (2)	Moderate (3)	Considerable (4)	Catastrophic (5)	
	Consequence of risk					

Thus, the significance of risk may be defined as:

$$\text{Sign} = \text{Like} \times \text{Cons},$$

where Like – likelihood, Cons – consequence.

Risks with the significance greater than 15 are unacceptable and require immediate response (“red” risks). Risks that have significance less than 4 are acceptable and determine the level of risk appetite of the company. Quantitative determination of the risk appetite according to the COSO ERM concept is the prerogative of the Board of Directors. “Amber” risks require control procedures. It should be noted that even the least possible catastrophic risk can be classified as “amber”, while the most likely insignificant risk is “green”, which means that it requires the development of additional guidance on the management of it held by internal auditors only if there will be available resources in Internal Audit Department. “Dark green” risks do not require any further action by management, and therefore they are not a subject of review by internal audit as they are within the risk appetite of the company.

4. The control procedures of internal audit

Risks should be assessed before and after consideration of internal control procedures. It results in the definition of inherent risk (IR) and residual (net)

register of risks, the auditors can only make some advice or recommendations in order to improve the enterprise risk management system. Risk register can be organized in a user-friendly form of MS Excel spreadsheet or MS Access database.

Critical analysis of foreign literature allows to identify four groups of risks that business usually faces with: strategic (risk of external economic environment and internal risks associated with the reputation and the strategy of the company), operational risks (business processes risk, human resources policy risk), financial risks (financing risk, trade and credit risks) and information risks (financial, operational and technological information risks) [13, p.117].

During the internal audit the auditors should check the documents confirming the company's objectives and risk assessment methods that were used by managers in order to build a risk register and the calculation of risk appetite. Taking into consideration these documents, the conclusion about acceptability of the developed risk register can be made.

Rather important is a concept of risk maturity, which affects the procedures of internal audit (Tab. 2).

Table 2

Internal audit procedures appropriate to different levels of risk management maturity

Level of risk management maturity	Internal audit features
Risk enabled to internal control system	For the internal audit purposes the risk register developed by managers is essential. The emphasis is usually made on timeliness of risk management. The Board of Directors is informed about possible risks
Risk managed	Internal audit is held. Internal auditors also assist managers in eliminating the insignificant drawbacks in the risk management system
Risk defined	Internal auditors can develop their own risk register based on the list of risks made by managers. The weakest areas of risk management are identified. Some interviews with the employees can be conducted. It can be given advice to managers about the management of individual risks.
Risk aware	The estimation of the quality of risk management is supplemented by risk workshop with managers to identify and explain the importance of identifying risks that are not realized.
Risk naive	

Source: developed by the authors on the basis of [8,10]

5. Risk and audit universe-planning

After determining the adequacy of the developed risk register and its ability to be the basis for planning the internal audit, it should be developed a risk and audit universe. The structure of this document is a logical continuation of the risk register. Risk and audit universe can be built according to the following structure (Tab. 3).

As we can see from the Table 3, in order to determine the significance of risks, internal auditors use the adjusted figure of inherent risks, that depends on the amount of time passed since the date of the last audit (gap) and risk assessment during the last audit on a scale "green-amber-red." Therefore, adjusted significance is calculated:

$$S_{adj} = S \times k_f,$$

where k_f – adjustment factor, that reduces IR,

which can be calculated using the information in the Table 4 [8, p.28].

So, not all risks listed in the risk register get into risk and audit universe: there is a kind of "filter" of risks. Selected risks can be grouped in terms of consequence, likelihood or operation cycles (deliveries, investments, production, sales etc.)

In order to develop the audit plan correctly it must be considered that the most risky areas (red) should be checked every year, amber - every 2 years, green - every 3 years.

6. The sequence of internal audit

The sequence of internal audit after the development of risk and audit universe and internal audit plan includes the following procedures:

1) identification of high-detailed list of company objectives and their relationship and consistency with

Table 3

Risk and audit universe – planning

Level 3 objective	Risk	Consequence of risk	IR			Last audit		IR _{adj}		
			C	L	S	Risk assessment	Year	Gap	k _f	S _{adj}
Sales on the conditions of commercial loan	Loan repayment delayed by the buyer	Financial loss	4	3	15	amber	2012	1	0,5	8
Buying the software for company purposes	Additional expenses on the adaptation	Financial loss, loss of time	4	2	8	green	2011	2	0,5	4
...										

Source: developed by the authors on the basis of [8, 9, 10]

Table 4

The matrix of adjustment factors of inherent risks

Gap		Adjustment factor of inherent risk		
		Green	Amber	Red
3	3	0,75	1	1
	2	0,5	0,75	1
	1	0,25	0,5	0,75
		Green	Amber	Red
Last audit risk assessment				

the objectives of the highest level and the overall goal of the company;

2) verification of the enterprise risk management system, review of the risk register and identifying the most risky areas. If there is no risk register or if there is a failure of risk management system, it is necessary to provide appropriate consultations to managers and, possibly, assist in the distribution of functions in the internal control system. It should be emphasized that internal auditors play an important role in monitoring risk management system, but do not have the primary responsibility to implement and support the functioning of this system;

3) internal control system testing. The higher the maturity level of risk is, the more attention to monitoring of controls by management should be paid. "Fieldwork" is the most difficult stage. Most of the control tests are carried out in the most significant risky areas identified in the audit plan and risk and audit universe. It is possible to conduct interviews with employees;

4) identifying areas where monitoring was not carried out considering the risk appetite of the company;

5) informing the managers about whether the risks were minimized to an acceptable level;

6) preparation of the Audit Report to the Audit Committee.

Foreign experience of internal auditing shows that the common practice after the internal audit is a meeting with managers of the company and discussing all residual risks detected that were above the risk appetite of the company. As a result of such discussion, the suggestions and recommendations on elimination or adaptation to the risks are made. The estimation of the possibility of achievement the company goals is held considering "green" "amber" and "red" risks. And of course, internal auditors provide assessment of efficiency and effectiveness of internal control system.

As the internal audit department serves the interests of the owners, the final document of internal audit is the Audit Report provided to the Audit Committee of the Board of Directors. The Audit Report by results of internal audit should include:

1) internal auditors' opinion on the timely identification, assessment and management of significant risks, on the effectiveness of internal control in terms of risk management with the obligatory indication of the weaknesses of the internal control system;

2) list of operational measures to be taken in response to deficiencies in the system of internal control to prevent possible losses;

3) data confirming the necessity for more detailed monitoring of internal controls;

4) assessment of the quality of performance the audit plan, that was agreed with the Audit Committee before holding the internal audit.

7. Conclusion

To sum up, risk-based internal audit is the most adequate model of the internal audit in the current economic circumstances. Its main difference from traditional approach to internal audit is in detecting and preventing risky situations in the operations of an entity and developing recommendations and suggestions to eliminate them. Internal auditing requires con-

centration of audit procedures to the high-risk areas. It can significantly reduce the number of required audit resources and increase the effectiveness of internal audit as a whole. An Audit Report is given to Audit Committee as a result of internal audit and consultations are provided to managers of the company in order to improve the risk management system. However, risk-based internal audit is fairly new to Ukraine and requires further development and active use by internal auditors of large companies.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дорош Н. І. Ризико-орієнтований внутрішній аудит / Н. І. Дорош // Матеріали 18-ї Міжнародної наук.-практ. конф. "Перспективи розвитку економіки України". – Східноєвропейський національний університет імені Лесі Українки (24-25 трав. 2013 р.). – Луцьк : Смарагд, 2013. - С.213-215.

2. Булат Г. В. Система внутрішнього аудиту в умовах глобалізації економіки / Г. В. Булат // Наука й економіка. – 2012. – № 4 (28). - Т.1. – С. 107-110.

3. Головач Т. В. Ризик-менеджмент: зміст і організація на підприємстві / Т. В. Головач, А. Б. Грушевицька, В. В. Швид // Вісник Хмельницького національного університету – 2009. – № 3. – Т.1 – С. 157-163.

4. Кулик Р. Р. Проблемні питання формування концепції аудиту і розширення ринку аудиторських послуг / Р. Р. Кулик // Вісник Львівської комерційної академії. – 2011. – Вип. 36. – С. 196–203.

5. Шалімова Н. С. Концепції розвитку аудиту: проблемні аспекти визначення та класифікації / Н. С. Шалімова // Вісник Донецького національного університету економіки і торгівлі імені М. Туган-Барановського. – 2009. – № 3. – С. 218–227.

6. Шухман М. Е. Методика планування робіт з внутрішнього аудиту на базі ризик-орієнтованого підходу/ М. Е. Шухман // Вісник Донецького національного університету економіки і торгівлі імені М. Туган-Барановського. – 2010. – № 3. – С. 367-375.

7. Benes V. Internal audit and it's approach to the risk mitigation / Ad alta: Journal of Interdisciplinary Research. – 2012. – Vol. 2, Issue 2. // [Електронний ресурс]. – Режим доступу: http://www.magnanimitas.cz/ADALTA/0202/A_benes.pdf

8. Griffiths D. Risk-based internal auditing: an introduction / D. Griffiths. – 2006. – 73 p. // [Електронний ресурс]. – Режим доступу: <http://www.internalaudit.biz/>

9. Griffiths P. Risk-based auditing. Gower Publishing Limited / P. Griffiths. – 2005. – 220 p.

10. Guide on Risk-Based Internal Audit. The Institute of Chartered Accountants of India. – 2007. // [Електронний ресурс]. – Режим доступу : http://220.227.161.86/2097_guide_risbbasedIA.pdf

11. Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements: 2012 edition // [Електронний ресурс]. – Режим доступу : <http://www.ifac.org/>

12. Internal Control: Integrated Framework – 2013. // [Електронний ресурс]. – Режим доступу: <http://www.coso.org/>.

13. Moeller R. Brink's Modern internal auditing. A Common Body of Knowledge / R. Moeller. – 7th ed. John Wiley & Sons Inc. – 2009. – 766 p.