Risks' Identification and Assessment in a Public Entity Regarding the IT Security Audit

Camelia Madalina BELDIMAN*

ARTICLE INFO

Article history:

Accepted April 2021

Available online May 2021

JEL Classification

H83

Keywords:

Types of risk, Strategic objectives, Level of risk, Table of strengths and weaknesses, Problems' analysis and fact sheets

ABSTRACT

This paper highlights the importance and inclusion in the Risk Register of the auditor's opinion regarding reaching of established goals, as well as the awareness of watching any risk that may lead to uncertainty, causing negative effects on those activities, by deteriorating the quality of expected results. Effective risk management assumes that risk identification is a permanent process, which allows the public entity to relate to the procedure of amendment and adaptation. For good risk management at all management levels, the directors of the departments at the first management level appoint those accountable for the menaces. They identify and collect the risks associated to the objectives and / or activities, assumed by the department head and monitor the implementation of risk management.

© 2021 EAI. All rights reserved.

1. Introduction

The risk is the hazard that an event or action will have a hostile impact on an institution's ability to successfully meet its goals. The risk constituents are the chance of occurrence as well as the level of the respective impact, the gravity of the consequences and their duration.

According to the General Rules on the exercise of the public internal audit activity, in Part II - Methodological rules on the public internal audit mission - in point 8.6.1. risk is defined as: "Risk is any event, action, situation or behavior with an adverse impact on the ability of the public entity to achieve its objectives".

Identifying the risks associated with each activity and operation is done by identifying all events, internal and external, that may affect in any way the performance of auditable activities. This stage differs slightly depending on the extent to which the audited institutions have so far identified their risks or not. In order to identify risks, the auditor uses questionnaires, question lists, quantitative and qualitative methods of analysis, groupings or verifications, comparisons, including staff interviews.

In the risk identification phase, it is decided which risks will be subject to audit. They are established both according to the level of operability of the operations or activities within the audited entity, and according to the presence or absence of internal controls.

The lowest risks correspond to the activities that proceed normally and are targeted by internal controls. These may usually be missing from the table of audited activities. A slightly higher degree of risk is represented by the operations that work, but have unstable results at internal controls, in which case it is recommended to perform the audit.

Next are those procedures for which internal controls are established, but they are not operational, which implies the existence of sufficient risks to be included in the analysis. The highest risk is found in the case of operations in which internal controls are not established and do not work.

2. IT Security Audit

A risk consideration is grounded on two evaluations:

- the degree of severity of the forfeiture that may result from the risk (or the direct and indirect effects);
- the probability that the risk will reappear (strictly quantified concept).

Hypothetical risks may turn up in audit suggestions, depending on the results of previous controls, tests, and verifications.

Strengths and weaknesses are uttered qualitatively and quantitatively depending on the anticipated results and the circumstances for obtaining them.

* Dunarea de Jos University of Galati, Romania. E-mail address madi.beldiman@gmail.com

A strength or weakness must be stated in terms of an internal control objective or an attribute chased, to guarantee the proper running of the audited entity / structure or the accomplishment of an expected result. From the activity carried out during the gathering and handling of information, the auditors proceed as follows: prepare a consolidated list of auditable objects; identifies the threats (risks) associated with these operations / activities; create the risk analysis criteria; establish the weight of each risk norm; establish the level of risks for each norm used; establish the total score of the norm used; ranks the risks based on the total scores attained; hierarchizes the tasks of the activities to be audited, respectively elaborates the "Table of strengths and weaknesses"; spread the "Table of strengths and weaknesses" and the outcomes made to the head of the Public Internal Audit Department.

The head of the Public Internal Audit Department coordinates a meeting to detect the audit purposes and risk analysis criteria. He re-evaluates the establishment of the objectives, the aim of the audit and the methodology, and consents the "Table of strengths and weaknesses" and the Problems and Analysis Sheets initiated for each prospective control.

At this stage, depending on the identification of the relevant risks, a table called "Identification of the risks associated with the auditable activities" is drawn up. The identification of the risks associated with each activity and operation is done by identifying all events, internal and external, that may affect in any way the performance of auditable activities. This step differs slightly depending on the extent to which the audited institutions have so far identified their risks or not. In order to identify risks, the auditor uses questionnaires, question lists, quantitative and qualitative methods of analysis, groupings or verifications, comparisons, including staff interviews.

The final result outcomes from the application at the assessment level of each of the three risk factors of some weights established according to the importance of the respective criterion, based on the following algorithm:

$$P_t = \sum P_i \times N_i$$

Where:

P_t is the total score

P_i is the share of risk assigned to each factor or criterion

N_i is the level of risk for each factor or assessment criterion.

Practice has shown that the way risks are assessed and managed has a significant impact on the ability of institutions to achieve their objectives. The internal audit activity in the field of risk analysis has beneficial contributions in terms of intelligent mobilization of resources, skills, and experience and at the same time develops the organization's risk management capabilities.

At the end of each assignment, the auditors prepare a reasoning, an evaluation of the quality of the internal control of the examined unit or system.

The evaluation of internal control is based on an analysis of the quality of the entity's internal control, on three stages:

- appropriate internal control;
- insufficient internal control;
- internal control with serious defects.

This consideration, made at the end of each audit engagement, is general referring to the audit engagement, and is the result of a joint debate between auditors.

The level of impact represents the effects of the risk in case of its incidence and can be uttered on a value scale on three levels:

- low impact;
- moderate impact;
- high impact.

The methodological norms illustrate the execution of the risk analysis by following the following phases:

- a) identification (listing) of auditable operations / activities, respectively of auditable objects. In this stage, the activities / operations as well as the current interdependencies between them are analyzed and identified, establishing the analysis boundaries;
- b) identification of threats, potential intrinsic risks associated with these operations / activities, by deciding their financial impact;
- c) establishing the risk analysis criteria. It is advised to use the following criteria: assessment of internal control, quantitative assessment, and qualitative assessment;
- d) establishing the level of risk for each criterion, by using a three-level value scale, as follows:
 1. for the evaluation of internal control: appropriate internal control - level 1; insufficient internal control - level 2; internal control with serious deficiencies - level 3;
 2. for quantitative evaluation: weak financial impact - level 1; average financial impact - level 2; significant financial impact - level 3;
 3. for qualitative evaluation: reduced vulnerability - level 1; medium vulnerability - level 2;

high vulnerability - level 3.

- e) establishing the total score of the criterion used (T). A weighting factor and a level of risk are assigned to each criterion. The product of these two factors gives the score for the corresponding criterion and the sum of the scores for a certain auditable process / activity leads to the determination of the total risk score of the respective process / activity;
- f) classification of risks, based on the total scores obtained beforehand, into low risk, medium risk, high risk;
- g) ranking the operations / activities to be audited, respectively the elaboration of the table of strengths and weaknesses. The table of strengths and weaknesses reviews the result of the assessment of each activity / operation / theme analyzed and allows the ranking of risks to guide the internal public audit activity, respectively to establish the topic in detail.

2.1 Use Case

To perform IT security audit operation, initially the audit team should build up a table like the one below.

Table 8. IT Auditable Objects and Risks

Domain	Auditable objects	Significant risks
IT	IT security policy	Absence of Security Policy Failure to enforce security policy in consistently
	Monitoring the implementation of the IT security policy	Absence of a designated manager to supervise the implementation of the IT security policy Failure to prepare and not methodically submit monitoring reports
	Evaluation of physical controls in IT	Absence of procedures for the implementation of physical controls in IT Failure to assign accountability for monitoring physical checks Absence of procedures for accomplishing physical checks
	Security of network access and data communication within the network	Absence of procedures for securing user access to the network Absence of the person in charge of monitoring the implementation of the procedures for safeguarding the user access to the network
	Antivirus programs	Absence of procedures for implementing antivirus programs Absence of the person in charge of monitoring the implementation of the procedures for implementing antivirus programs Failure to perform regular monitoring
	Data disaster recovery	Absence of data disaster recovery procedures Absence of the person in charge of monitoring the implementation disaster recovery procedures Failure to perform systematic monitoring Failure to take the necessary measures to recuperate data in case of disaster according to the procedures
	Archiving system	Absence of data archiving procedures Failure to assign accountability for data archiving Failure to perform the periodic assessment of the archiving activity

Risk identification is the second document that is developed within the Risk Analysis procedure and involves the association of significant risks with the operations established in the Centralized List of Auditable Objects. Usually, one or more possible risks are associated, determined by the internal auditors based on the information collected but also from the practical risks arising from their own experience. If several audits are attached to the auditable operations, their analysis can be performed for each risk separately or on a total auditable operation / object.

For the current use case, the audit team managed to rank the 7 auditable operations as described in Table 2.

Table 2. Classification of Operations According to Risk Analysis

Domain	Auditable objects	Total score	Ranking	Remarks
IT	IT security policy	2.3	High	
	Monitoring the implementation of the IT security policy	2.0	Average	
	Evaluation of physical controls in IT	2.5	High	
	Security of network access and data communication within the network	2.3	High	
	Antivirus programs	2.0	Average	
	Data disaster recovery	2.1	Average	
	Archiving system	1.7	Low	

Low risks 1.0 - 1.7

Average risks 1.8 - 2.2

High risks 2.3 - 3.0

After finishing the evaluation process, to amend the activity carried out and to remove the deficiencies found, the following suggestions were elaborated by the audit team:

- Establishing a risk management strategy at the public entity level;
- Establishing those responsible for the elaboration and systematic updating of the procedures regarding the elaboration of the Risk Register;
- Validation of the attributions and responsibilities from the procedures with those from the job description regarding the risk management;
- Organizing and keeping up to date the Register of risks incorporating the internal control measures that are taken to restrain them;
- Systematic monitoring, at the request of the manager accountable for administrative issues, of the manner of noticing in the daily activity the written and formalized procedures meant to ensure the risk management;
- Training the staff to complete the Risk Register by the person in charge of keeping it;
- Notifying the team of auditors about the stage of elaboration, taking ownership and monitoring of risks.

3. Conclusions

This internal audit report was formulated built on the Centralized List of Auditable Objects, the Audit Program and the On-Site Intervention Program, the discoveries made during the gathering and processing of information, and during fieldwork. All outcomes are based on audit evidence obtained based on the tests recorded in the working documents (checklists, worksheets, interviews, report notes) prepared by internal auditors and grasped by the management factors of the entity.

The evaluation is based on the debates that took place, regarding the suggestions of the internal auditors, in the closing session of the mission, esteemed by the participants as accurate and achievable.

Also, we consider that the outcomes of the assessment of the internal auditors regarding the IT Activity are in normal limits for this period of implementation of the information technology function in the public entities.

Therefore, we appreciate that, by carrying out the suggestions of the internal audit team, the IT activity will experience a significant enhancement.

The audited entity has the responsibility to prepare the Action Program in order to implement the suggestions and to report to the team of internal auditors, periodically, their implementation stage.

References

1. Ghiță, M., and all (2009), "Guvernanța corporativă și auditul intern" (Corporate governance and internal audit), Editura Aeternitas, Alba-Iulia, pp. 354-368.
2. Mares, G., and all (2007), "Practica auditului intern privind fondurile publice naționale și ale Uniunii Europene" (The practice of internal audit on national and EU public funds), Editura Contaplus, Ploiești, pp. 211-226.
3. Morariu, A., Suci, Gh., Stoian, F. (2008), "Audit intern și guvernanță corporativă" (Internal audit and corporate governance), Editura Universitară, București, pp. 157-178.
4. Oprean, I. (2010), "Control și audit intern, suport de curs pentru masterat" (Internal control and audit, course support for master's degree), Universitatea Dimitrie Cantemir, Facultatea de științe economice, Cluj-Napoca, p. 120.

5. Oprean, I., Popa, I.E., Lenghel R.D. (2007), "Procedurile auditului și ale controlului financiar" (Audit and financial control procedures), Editura Risopront, Cluj-Napoca, pp. 110-134.
6. Tiron, A., Gherasim, I. (2015), "Auditul intern în instituțiile publice" (Internal audit in public institutions), LGA Romania.
7. Zinca, C.I., Petroianu, G.O. (2017), "Rolul auditului intern în managementul riscului instituțiilor de credit" (The role of internal audit in risk management of credit institutions), Revista ECONOMICA, no. 3 (101), pp. 102-103.
8. "Procedura de lucru privind desfășurarea misiunilor de audit public intern de asigurare" (Working procedure for carrying out public internal audit missions), Universitatea din Pitești, 2017