INFORMATIONAL RISK AND NECESSITIES AUDIT

Inga, Bulat [1]

Summary

We are living in an informational era where the changes and challenges are very complex and at high speed. The informational system has become a premises for starting a new day. Its presence within the activity of a certain institution is more and more dispensable.

Nowadays the auditors have a very important role in studying the systems, the processes, the mechanisms, etc, so that the approach in offering recommendations is the result of everything that is going on and which can generate. The audit activity is external, independent, but human, thus it cannot lack risks. The risk associated to the audit activity, considered as being an inherent, checking and residual risk, brings forward to the user that the accountant information which is validated by means of audit cannot itself lack risks, so we can notice a direct relation between the audit risk and the risk associated to the information given publicly by entities. That is why, the tendency which the audit societies must follow is to manage as efficiently as possible the risks afferent to these activities, which for them, is becoming a risk of an economic origin.

Key words: risk, audit, auditor, information, control, system, institution

Classification JEL: M15, M42

"An unseen point yesterday, is a target today and will be a starting point tomorrow"
Maclaulay

1. Introduction

The analysis of risks or barriers makes us stress on various criteria, in order to be able to make a more ample analysis referring to the next day. Beyond its regulation, nominalization and standardization, the information of the internal control requires an approach from the qualitative point of view. In this way, the control sufficient up to a certain moment has become insufficient to guarantee the reliability of the information which is relevant. In these circumstances, an external and independent validation of the relations and the plans given publicly by the operational managers is imposed. In this way the internal audit responded to an acute need of validating the information presented by the institution internally and externally as well.

1.1.The management of risks in the audit framework

Some risks are acceptable and unavoidable referring to different activities, but there exist unacceptable risks, too. The purpose of each institution is to avoid as much as possible the unaccepted risks and to mention at a tolerant level the accepted risks to achieve the proposed objectives.

The audit objectives is to evaluate the risks of the internal controlling system up to detecting the frauds, a process which implies a more detailed checking of all the processes and the systems of internal control, by means of risks.

Thus, the degree in which the information reflects the correctness of applying the mechanism is determined, but the auditor's efforts are intensified to identify the further manipulations with the information offered by the system of internal control in order to avoid the cases of errors and frauds.

The information offered by the specialists in the field are necessary for all the categories of staff.

[1] Doctorand, Institutul Național de Cercetare Economică din Chișinău, bulat.inga124@gmail.com

For this reason the results of the audit works must be correct and well made being based on the legal documents in force. They must assure the quality and coherence of the system of internal control and are meant to reflect correctly, fairly and completely the described processes. At present there are more types of audit missions:

a) *the system audit* , which examines the system of financial management and control to estimate the efficiency of its functioning;

b) *the compliance audit*, which verifies the procedure of the legal framework, the applied policies and, if the case, the need to improve the internal checking procedures used to insure the compliance with the legislation;

c) *the financial audit*, which estimates the adequate and efficient functioning of the internal checking procedures afferent the financial systems;

d) *the performance audit*, which examines the use of the resources within a programmer, functions, operations or management system to determine if the resources are used as economically and efficiently as possible to achieve the institution's goals.

e) *the informational technologies audit*, which examines the efficiency of the financial management and the control of the informational technologies.

The analysis of risks implies a process of identification of the main risks, stating the amplitude and involving the risks, as well as identifying the segments which present a great risk and which must be monitored. The risk analysis is made a part of the whole measures which is generically called the management of risks. The evaluation of the informational risks implies a process of a more detailed analysis of risks that must be done for more reasons:

1) Identifying the primary objectives of the institution regarding the realization of its visions;

2) Creating some following stages in getting rid of the conditions which can contribute to the appearing of some risks when the context is complex, but an alternation of its functioning cannot be applied but by means of small steps policy;

3) Stating the compulsiveness of some actions and of some deadlines to create some objectives which deal with the implementation of the recommendation given within the audit missions;

4) Creating a perspective of a whole of acquiring resources and services so that the financial effort to be taken into account regarding the fact of finding the most efficient solutions;

5) The analysis of the controlling programmer with the institution's mission;

6) It offers more detailed evaluation criteria of some processes or system of control.

Every audit mission implies risks, but their identification , at the stage of planning the work, is one the most important objectives of the audit. We must state that this is a very difficult activity and it does not offer any full guarantees. To provide a result regarding the level of the risks, first of all, it is necessary to identify them.

The National Standards of Internal Audit take into account tree most important categories of risks: *the inevitable risk, the risk of control and the residual risk.*

The risks of control present the inequalities and the errors that are not discovered with the inefficient control. The evaluation of these risks is made depending on the used informational system, on the way the system of control is organized, on the way the procedures are organized and applied. The risk of control cannot be equal to zero, because the internal control cannot offer guarantees as to prevent or to detect the errors. The auditor cannot change the level of the control, he/ she can only "influence" it through recommendations of improving it, but this influence will only be seen in later audit periods and only following the circumstances in which the leadership will take into account the given suggestions.

The inevitable risk and the risk of control are independent of the auditor's activity and cannot be checked by him, but they can be estimated and they determine the basic procedures that will maintain the residual risk at an acceptable level.

The residual risk presents the risk as a basic procedure of an auditor not to detect a mistaken information, which could be significant in an individual way, or when it is combined with wrong information from other sources. The level of the residual risk is directly connected to the procedures used by the auditor. In comparison with the inevitable risk and the risk of control, the residual risk can be checked by the auditor by:

- auditor's adequate planning;
- corresponding stating of the sample type;
- identifying and evaluating the performances of the quality insurance;

Estimating the risks in the audit system is a complex activity and there is no agreement yet about how the problem should be treated. Practitioners use mostly the model given by the national standards of internal control, though this one is often criticized in literature, the main arguments against it are the simple way by which the issue is approached and the inability to meet requirements of all the auditors. On the other hand, the probabilistic models are often much more complex and need deeper knowledge from other fields like; Maths, Statistics, etc. Anyway, they witnessed a great development during the last years, especially in the legal framework. A solution for this problem is the software development which, theoretically and probabilistically based, should offer the practitioners easily used solutions and give a correct evaluation of the risks in the audit and not only. This would lead to overpassing the subjectivity which at present characterizes many audit missions and would ,somehow, set the auditor free from the charge of estimating the risk using only his own experience and knowledge. Thus, the interpretation and the presentation of the audit risks by probabilistic methods offers another perspective of the way this issue can be solved, an objective and more precisely a problem concerning more specialists from this filed.

The biggest part of the administrative and operational functions of the institutions is conducted at present with the help of the informational systems, which is necessary that the audit system be well-equipped. Within the audit missions, various methods to evaluate the internal control systems and the risks that can threaten these systems will be used.

II. Evaluating the risks in the system of computer information

One of the most important problems in auditing the electronic systems is evaluating the risks and the system of the internal control. That is why, in planning those four audit components, the auditor must get an understanding of the meaning (materiality) and the upper complexity of the activity of the informational computer systems (further on ICS) and of the data availability which is used in the audit.

The nature of the risk and the features of the internal control on the average ICS includes: (5:52)

a) *the lack of evidence regarding the operations* Some ICS are so created, that some full evidence useful in audit regarding the operation, can only be for a period of time or just in an electronic way, due to the great number of processing steps;

b*) the uniform processing of the operations.* The computer processing works out uniformly similar operations, based on the same instructions of processing. In this way, the errors of editing documents which are at the basis of the operations and which as usual were associated with the manual processing, are virtually eliminated. On the contrary, the errors of programming (or the errors in hardware or software) result in working out incorrectly all the operations.

c) *the list of separation of functions.* Some procedures, which normally are done manually by different persons, in ICS can be concentrated in such a way that a person who has access to the programs, procedures or computer data could perform incompatible functions.

d) *the possible appearance of errors and inequalities.* The probability of appearing of human errors in developing, maintaining and exploiting ICS is bigger than manual processing. There is a greater possibility that some persons get unauthorized access to data or even to alter data without visible evidence than in the SIC medium. Diminishing human implication in ICS can diminish the notice of errors and inequalities.

e) *initializing and executing some operations.* In an ICS medium, the computer's ability to initialize and execute automatically some operations can be included. These operations can not necessarily be so documented as in the manual system, but the manager's authorization regarding these operations can be implicit by way the computer system was designed.

f) *the dependence on other controls by computer processing.* Computer processing can produce reports and data that are used in making the manual control procedures, whose efficiency depends in this way, on the efficiency of the controls over the completeness and the precision of the computer processing.

g) *raising the degree of the manager's supervision.* An ICS medium offers the institution's administration a large variety of analytic tools which can be used to supervise the operations, in this way enhancing the activity of the whole internal control team.

h) *raising the degree of using computer assisted audit technics.* The use of computer in processing and analyzing a big amount of data can offer the auditor the possibilities of using computer assisted audit technics. The inevitable and control risks are limited in evaluating the systems of control, that derive from (5:54)

- ✓ developing and maintaining the programs;
- ✓ supporting the software systems;
- ✓ the types of processed operations;
- ✓ the physical security of ICS;
- ✓ the control over the access to the used programs;

The subjective evaluation of risks will lead to the increase the potential of error appearance and of the fraudulous activities in applications, data base or files and other processing activities.

III. The evaluation and the management of the informational risks in IT audit.

Starting from the idea of having limits in the audit system, more stress on the significant identification corresponding to all deeds, activities and events is recently put. Every manager has to find the solution, on the one hand, to manage the threats, otherwise, he would disqualify and on the other hand, to fructify the opportunities to the benefit of the institution proving this way its efficiency.

The risk is the event able to exercise an influence on performing internal audits in the IT system or monitoring the processes in an initially created way. Most of the mangers focus more on the analysis of risks to overpass the crisis and to lower the losses. Every auditor in analyzing the risks state different criteria of quantitative and qualitative evaluation of risks.

Depending on the fields that are monitored the financial losses are taken into account too. More often, the complexity of the risky factors is conventionally divided into objective and subjective. The objective factors focus on : changing the data of the beneficiary conditions, late providing of information, the force major circumstances; but those subjective include: characterizing the mutual relationships between the beneficiary and the audit team, so everything that refers to the so-called" human factor".

Another premises to make an analysis from where the challenges or the threats may come by means of ecosystem, can categorize the risks into those internal and those external. For a good functioning of the IT system it is important to remember that there are risks: ratable and not evaluable depending on the circumstance or on the vulnerability of the situation we are in. The risks and the threats are identified, usually mutually. They discuss about a risk and they infer implicitly the threats that can be produced by that risk. Risk is a more abstract notion than the threats that implicitly refer to the costs of implementing the respective threat, intuitively and the quantification of the effective realization of the threat.

The evaluation of the informational risk is an approach for the internal audits, because the uncertainty represents a daily reality, respectively, the reaction to the uncertainties must become a permanent preoccupation. The computer, the information technologies and the communication have dematerialized the financial information and have ensured the rise of possibilities of rapid gain as well as the global circulation which enhanced the possibilities of manipulation of it by issuers as well.

The analysis of risks is meant to help the realization of the audit on theoretical basis and solid practices. The risk approach distinguishes by:

1. the quantitative analysis
2. the qualitative analysis
3. the analysis of every workstation within the system;

***<u>The quantitative analysis of the risk implies the following stages</u>*:**

Identifying and evaluating the assets- the hardware, software components, the operating data, the staff involved in the process, the afferent documents, the respective support, etc. We must take into account the analysis and the calculation of the cost of the workmanship during the intervention; the time needed to state the cause of the malware; the duration of the loading and the testing of the application, the period of restoration, recharging the big application systems. As for the staff working with these processes, the main criteria that can be grouped around them are: the amount and the qualifications of the personnel, the costs of additional instruction, the psychological effects of the disasters;

Determining/ stating the vulnerability- implies stating the threats towards the activity and the frequency they can produce: natural, accidents, intentional acts. The impact of these threats depends mostly on certain factors, of which most of them are: facilities for the organizing framework, information density, the local economic conditions, the warning and protection implemented systems, the visibility, the easy access to the assets, methods and procedures of saving, acknowledging the security and protection measures.

Estimating the probability of producing an incident- sating the probability of producing an incident in a short period of time, well-estimated, using statistic data which can fix the rate of producing an incident. The calculation of the annual estimated losses- each threat is calculated.

$$PAE_b - \sum_{j=0}^{m} Vb\ Ea \qquad (1)$$

where **PAEa**= annual estimated losses for threat **a.**

Vb= the asset value **b** (being assets labeled from **0** to **n**)

Ea= estimating the number of incidents and threat **a** (there taken int account the treats labeled from **0** to **m**)

The annual estimated losses can be calculated by: categories of assets and threats or major pairs of assets/ threats.

✓ *Determining the main measures of preventing and control- the major losses and threats are put at its basis.*

The calculation of estimating the ratability of the infestation (RI)- it is calculated to identify the cost of an applied control: *the vulnerability, assigning a rate/ value optimal for every event/ way of controlling, estimation the annual costs for implementing the measures of the respective control. (11)*

$$(RI): RI = rc \cdot PAE_a \quad Cc \quad (2)$$

Where we operate with the notations:

Cc= the annual cost for applying the control **c**

Rc= the efficiency indices for the control **c**

PAE= Estimated Annual losses for the threat **a**

Choosing the additional measures of control must be bases on the following objectives: the bigger Value of Ratability of the Investment and minimizing PAE.

The bigger factor's value **RI** will be obtained acting upon the indices of rentability **Rc** by raising it up to its maximum value 1, or upon the annual cost for applying the control **Cc** by diminishing the costs of implementing the control. The quantitative method lack something:

- *-The difficulty in finding a number which quantifies more exactly the frequency of producing an event;*
- *-The difficulty in quantifying certain values;*
- *-The methods does not distinguish between the big or small threats, it characterizes the financial effects in the same way;*
- *-The choice of the used numbers can be considered subjective*

The qualitative analysis of the risk- is more often used by smaller institutions, where the analysis of the risk is not conducted on basic statistic data, but it uses the incoming and outgoing documents and the estimated losses. Even more often they operate with the terms: often/ high, average, rarely/ reduced- referring to the probability and the impact; vital, critical, important, general and informational- referring to the type of classification; numbers 1, 2, 3.

While conducting audits it is useful to use the quantitative and the qualitative analysis of the risks as well. The qualitative analysis is more often used to state the objectives of the analysis of some processes, systems, etc

The quantitative analysis of the risks is used when we are based on documents or on the sums, which are estimated while stating the evidence of evaluation of the system that undergoes the studies.

Thus, we will be able to state what the greater risks from the controlling system's side are of the informational system or of any other process.

The analysis of every workstation within the system- it is a more ample analysis at the basis of which are both the qualitative and the quantitative analyses. It is much more expensive and needs more time. At present it is being used mainly by bigger companies.

Concusion: The informational era already implies a penetration in various fields and a complexity in stating the risks within the audits.

The audit of the informational systems is not an isolated audit, but it is based on the analysis of systems in the administrative activity. Today the informational applications are a set of administrative, financial programs, etc. which create a system of operating and monitoring of the institution's activity.

The challenges and the tendencies of the modern society leads the audit to fixing the limits of the internal audit by means of analyzing the acceptable internal risks as well as the

external ones. According to the analysis of all the types of information frauds and errors will be prevented as well as the diminishing of the risks in realizing the objectives, which will lead to new changes or transformations imposed from the outside of the institution.

Bibliography:

1. Anghel, I., Oancea Negrescu, M., Anica Popa, Ad., Popescu A.M., (2010), Evaluarea întreprinderii, Ed. Economica, Bucureşti
2. Botnari, N., (2008), Finanţele întreprinderii, Ed. Prim, Chişinău
3. Ghiţă, M., (2009), Auditul intern, Ed. Economica, Bucureşti
4. Ghiţă, M., (2008), Guvernanţa corporativă, Ed. Economica, Bucureşti
5. Ghiţă, M., Mareş V., (2002), Auditul performanţei finanţelor publice, Ed. CECCAR, Bucureşti.
6. Horomnea, Em., (2014) Audit financiar. Concepte. Standarde. Norme, Ed., Tipo Moldova, Iaşi
7. Paşcu, A.M.,(2014), Calitate şi responsabilitate în audit şi profesia contabilă, Ed., Tipo Moldova, Iaşi
8. *** Ministerul Finanţelor al Republicii Moldova, (2013), Manual de audit intern, Chişinău,
9. Legea nr. 229 din 23.09.2010 ”Privind controlul financiar public intern” Publicat în Monitorul Oficial Nr. 231-234 art Nr : 730 din 26.11.2010
10. ***Ordinul Ministerul Finanţelor nr. 189 din 15.11.2015 ”Cu privire la aprobarea Standardelor naţionale de control intern în sectorul public” Publicat în Monitorul Oficial Nr. 332-339 din 11.12.2015,
11. *** http://www.securitatea-informatica.ro/