THE INTERNAL AUDIT CONTRIBUTION TO KNOWING AND IMPROVING RISK MANAGEMENT OF ECONOMIC ORGANIZATIONS

Cristian Virgiliu RADU, PHD Student
General Manager, Recopal Limited SRL
crradu@hotmail.com

Abstract: *The notion of audit comes from the Latin auditum as an obedience, then an investigation, and ultimately a suggestion of solutions, the audit allowing the contribution of value to the reasoning of a motivated and independent person. Audit is the process by which competent, independent individuals collect and evaluate evidence to form an opinion on the degree of correspondence between those observed and certain predefined criteria. The audit term is fashionable. Fashion may pass, but the need for competent and independent evaluations in various areas is growing. As an examination, in order to determine the properties of a representation, the audit first applied to financial representations. There is financial audit, investment audit, marketing audit, quality audit, audit of information systems, IT, office, and social audit.*

Keywords: *audit, risk management process, organizations*
JEL Classification: M42, G11, G30

Introduction

Like each of us, organizations set goals that target different time horizons: short, medium and long. At the same time, any goal, irrespective of the time horizon it refers to, is subject to events that could jeopardize their realization. The importance of risk assessment of an entity is marked by both

the negative impact that can be avoided by developing a protection policy and the probability that can be avoided by developing a preventive policy.
The word "risk" derives from the Italian word "risk" that means "dare." Thus, we can say about this concept that it is "a choice, not a fate".

Any activity we undertake carries risks that materialize with or without our will in one sense or another. The ideal is to perceive them as they are and to use them for our benefit.

Under 2120.A1[1], internal audit evaluates the exposures to risks associated with the governance of the public entity, its operations and its information systems with regard to:

- the veracity and integrity of financial and operational information;
- the effectiveness and efficiency of operations and programs;
- protecting heritage;
- compliance with national laws, regulations and regulations.

There are several types of risk in practice, classified according to certain criteria.

- After the probability of occurrence, the risks are:
  - potential risks likely to occur if no control is in place to prevent or correct them;
  - Possible risks, represented by those potential risks for which management has not taken the most effective measures to eliminate or mitigate its impact.
- By their nature, the risks are:
  - Strategic risks, related to mistaken actions related to organization, resources, environment, IT endowment, etc.;
  - information risks related to the adoption of unsafe or unreliable information and reporting systems;
  - Financial risks, related to the loss of financial resources or the accumulation of unacceptable liabilities.
- By nature of the activities (operations) carried out within the entities, the risks are:
  - a legislative risk;
  - a financial risk;

1 Order on the approval of the National Internal Audit Standards no. 113 of 10.12.2012 published in the Official Gazette no.237-241 / 1378 of 16.11.2012

- operational risks;
- commercial risks;
- a legal risk;
- a social risk;
- a picture risk
- environmental risks
- information security risks, etc.

The risk management department, where it is organized, has the task of managing the risks that may arise within the entity and, potentially, the impact it may have on achieving the entity's objectives.

According to the specifics of the entities, the risks are:

- general risks, regarding the economic situation and the organization of the management;
  - Risks related to the nature of specific activities (processes, operations);
  - Risks related to the design and operation of systems;
  - Risks related to the design and updating of procedures.
- According to the General Norms regarding the exercise of the public internal audit activity, the risks are classified as follows:
  - organizational risks, such as: non-formalization of procedures; lack of precise responsibilities; insufficient organization of human resources; insufficient, outdated documentation;
  - operational risks, such as: not recording in the accounting records; inappropriate archiving of supporting documents; lack of control over high-risk operations;
  - financial risks, such as: unsecured payments, non-detection of financial risk operations;

Risk management has the task of continuously reviewing the organization's activities to identify new risks or how they have evolved over time. At the same time, the risk management department develops and updates the organization's rules and procedures regarding internal control to be implemented[2].

Internal auditing is not the same as internal control, even if we consider the incompatibility of the two functions: you cannot monitor and

2 Domnişoru S., Vînătoru S. (2008).*Internal Audit and Control*. Craiova: Sitech Publishing House.

evaluate objectively and independently what you do. Through internal audit, the management of an organization seeks to ensure that the internal control function in place functions efficiently, effectively and sufficiently to improve or eliminate the identified risks.

The role of audit in the risk management process

The quality of internal auditor requires that a risk-based approach be used in the preparation of an annual audit plan. In fact, professional standards specifically require this. For a good risk assessment, the auditor needs to know the entity, auditable activities, associated risks, and internal control activities that work.

Risk assessment is a permanent issue, as conditions change forever, new regulations emerge, new people appear, topicality emerges, and all these changes constantly change the risk management process, which can never be completed.

In our view, our internal risk-based audit is defined as the activity that provides assurance on risk identification and management by the management structure. The responsibility of internal audit in risk management is underlined even by the definition of internal audit. By examining this responsibility, we have obtained the following conclusions on the role of audit in the risk management process:

- The audit adequately establishes the techniques and procedures only if it is based on sound knowledge of the risks faced by the entity, therefore knowing the risks and their effects is a research scope for the auditor, knowing these risks is designed to help the auditor place the entity in an area or other risk.
- Not many risk factors are important, but the auditor's knowledge of the risk as such, the way in which it acts, the factors that drive and maintain it in a favorable environment, as well as the factors that can direct it to disappearance.
- The importance of risk management arises from the responsibility of management to design and implement an internal control system that performs the legal and effective management of the risks associated with the activities carried out within the entity.

As a consequence, internal audit is designed to provide assurance to the entity's management of the functionality of the internal control system and of the quality of risk management.

Some organizations, especially the large ones, have created a distinct operational structure to carry out this complex process, known as the organization's risk management (ERM). At the same time, given that economic and legislative circumstances are constantly changing, new mechanisms are needed to identify and control the risks associated with these changes.

The internal auditor, from the moment when the activities leading up to the audit engagements are carried out, and until they are completed, will deal with the risks. Risk is any element that may have an impact on the organization's ability to achieve its goals. This may include deprivation of liberty in the sense that internal auditors cannot do anything.

In conjunction with the publication of the Enterprise Risk Management-Integrated Framework (COSO), the IIA has issued a guide to the heads of audit departments presenting recommendations on internal audit relationships with ERMs within their organizations[3].

Among other things, the purpose of this guide is to establish a clear line of risk management and internal audit responsibilities vis-à-vis the two.

Thus, the main internal audit activities in relation to ERM are:

- providing assurance on risk management processes;
- providing assurance that the risks are being correctly assessed;
- evaluation of risk management processes;
- Evaluating reports on critical risks;
- Essential risk management analysis.

Regarding the legitimate role of internal audit, the IIA emphasizes:

- facilitating the identification and assessment of risks;
- advise management to take risk protection measures;
- coordination of ERM activities;
- trengthening risk reporting;
- maintaining and developing the ERM framework;
- Developing the risk management strategy subject to approval by the Board of Directors.

At the same time, the IIA warns about the roles that internal audit should not assume:

- establishing the appetite for risk;

3 Renard J. (2002). *Internal Audit Theory and Practice*, Paris: Publishing House, Translation Ministry of Public Finance, Bucharest 2003.

• imposing risk management processes;

Auditor's knowledge of the accounting and internal control system allows effective planning and development of an audit engagement as it will have implications in assessing the control risk and procedures to be used to reduce the risk of the mission at a level acceptable minimum.

Starting from this fact, in a personal sense, the role of internal audit in risk management is to provide a permanent information flow to identify and analyze the risks relevant to achieving the objectives and to provide reasonable assurance as to the extent to which the objectives can be achieved. Within this information flow, we consider that the role of internal audit differs according to the moment of risk reporting as follows:

- If the risk assessment is carried out before its effective occurrence, the role of internal audit is to analyze the sufficiency of internal control to avoid that risk;
- If the risk assessment is carried out after the risk has been detected as an actual product, the role of the internal audit is to determine the causes that have led to the risk exposure and to propose internal control measures for elimination, in order to ensure that the organization's objectives are met.

Thus, the internal audit has the possibility and the task of forming a self-evident, informed and independent view of the risks faced by the economic organization and to communicate directly the points of view, findings and conclusions to the hierarchical body and / or management, supporting superior leadership in effective supervision and achievement of established goals. Collaboration between internal audit and risk management functions creates synergy, generates added value through mutual pooling of resources, skills and experience, and develops the organization's capabilities in risk management.

Models of quantitative and qualitative risk assessment

Risk analysis is not an exact science. By establishing the control activities, the high risks are to be averaged or low, until eventual disappearance. However, the risks have to "evolve" downwards. The literature discusses two models of risk value analysis: the quantitative model and the qualitative model.

These start from the premise that any organization can expect to lose losses due to the inefficiency of a computer system, and this risk of loss results from the impact that threats on the organization's resources pose.

The quantitative model is based on the following elements:

- the credible asset value of the assets;
- the probability of annual losses;
- the expected annual loss;
- cost of control and precautions
- uncertainty.

The impact of one single threat or the potential loss associated with a single occurrence is calculated as follows:

Impact = FV * VA or PPA = FV * VA

The annualized loss is influenced by the annual rate of occurrence of the risk and can be determined as follows: PAA = PPA * RAA

where:

FV - vulnerability factor

VA - asset value

PPA - the potential loss associated with an occurrence.

PAA - Early Yearly Loss

RAA - annual rate of occurrence

Such an analysis also includes a cost / benefit assessment that will facilitate the design of the return on investment (ROI) for a given set of controls.

ROI = Net Benefits / Cost

These mathematical models provide a concrete result, but must be included in the economic environment and noticed if it represents reality.

Internal auditors can carry out accurate and complete evaluations when they have concrete facts or elements, but as a rule, when they intervene it is late because the facts have occurred and the problems have already arisen. This is where the novelty of the internal auditor's work, namely to act before the risk-producing phenomena, comes in. For this, a horizontal approach must be taken to raise the interest of the auditee, to be responsible for the risks it manages. An important element here is communication after the completion of internal audit activities.

Specialist Alan Oliphant, as shown below, proposes a qualitative risk-assessment model that takes into account basic factors in assessing the value of the risk: financial impact, vulnerability, complexity and trust:

In this case, the value of the risk will be expressed by the values

"Very Low, Low, Medium, High, Very High"

and not in absolute values,

and the formula for determining the value of the risk is as follows:

VR = VF * [(Cv * Wv) + (Cc * Wc) + (Ct * Wt)]

where:

VR - risk value

VF - financial impact on the organization; it represents a potential cost of the organization in the event of an error, system failure, fraud or other negative events.

The material value will be given by the financial value or the value of the assets. The impact on the organization can be increased through a non-financial multiplier:

[(Cv * Wv) + (Cc * Wc) + (C1 * Wi)]

where:

Cv-vulnerability refers, on the one hand, to the way authorized users have access to the system, and on the other hand, the accessibility of the organization's system and assets to unauthorized users.

Cc - the complexity, takes into account the risk associated with the information technology itself, the number of users in the compartments or in more generic terms the organizational complexity.

But - trust, reflects human behavior in the organization and addresses two aspects: the integrity of staff and the level of involvement of managers.

and, Wv, Wc, Wi - are weight factors (important) that can be applied at the auditor's discretion, depending on the specific conditions.

The accessibility of an information system can be evaluated according to the physical restrictions implemented within the organization and the modalities of access through the communication network. The calculated risk value will be translated into a "translation table" indicating the level of risk; in the design of this table, the auditors take into account the following rules:

1. the lowest risk value = 0 and

2. the highest value is considered to be the total (financial) value of the organization multiplied by 3.

Risk analysis or assessment is an important step in the work of auditors and is carried out for: the preparation of the audit plan and the preparation of the audit program, becoming an essential part of the management that must be carried out constantly at least once a year to identify all risks. It comprises the following phases:

a) identification of auditable objects (elements), which involves a structured approach starting from general to detail

b) establishing the risks for each auditable subject on the basis of the analysis of operations according to certain pre-designed criteria and performing hierarchical calculations and ranking them;

c) risk measurement, which will be based on the likelihood of occurrence of the risks and the impact and duration of the event's consequences.

Risk measurement is done through three methods:

• the probability method, which involves the following steps:

- assessing probable losses based on statistical tools and a historical approach;
- Direct valuation of annual losses;
- recognition and extrapolation, with corrections, if necessary.

• the risk factor method, which is identified in advance from a risk classification.

• method of appreciation matrices, based on the criteria of appreciation and weights

risk on:

- financial impact: I - 35%;
- probability of occurrence: P - 20%;
- level of internal control: CI - 45%

The dimensioning of the relevance of the risks (R) is done through the two components variables of each risk: the consequence (C) and the probability of occurrence (P).

Arithmetically, the calculation relation is expressed as: R = CxP

We recall that if there is a risk management department within the organization, this assessment would be the responsibility of the organization.

Risk assessment involves identifying and analyzing them in light of the perceived threat to the organization's objectives as part of the operational process that needs to identify and analyze internal and external factors that could affect the organization's goals.

Internal factors may be, for example, the nature of the entity's activities, staff qualifications, major organizational changes, or employee performance, and external factors may be the variation in economic, legislative or technological changes.

Financial impact is defined as the value estimate of entity losses as a result of exploitation of system vulnerabilities by threats. This impact can have two components: a short-term impact and a long-term impact.

Risk assessments must cover the whole range of risks within the entity, so work should be done at all hierarchical levels, especially at the highest levels.

The evaluation process should identify measurable risks and non-measurable risks, such as operational risks, and select those that are controllable.

Management, through predefined control activities, identifies the risks and analyzes their evolution at the organization level. The Internal Audit Department, being an independent structure, resumes management risk analysis to assess the internal control system.

Internal auditors should report to management general results of their work and any significant weaknesses discovered during the course of the audit.

However, auditors are at their own risk: audit risk.

They should consider the audit risk at the individual, balance sheet or transaction class. This helps them outline the audit area and set audit procedures.

The risk management process involves several steps, namely:

- identification of activities, operations;
- identifying the risks associated with them;
- establishing risk factors or criteria;
- risk evaluation;
- risk hierarchy or prioritization;
- the establishment of an owner, the person in charge of risk management;
- defining an action plan and tracking its implementation;
- systematic reporting of implementation of the recommendations.

Risk assessment is a concern of both internal auditors, which they perform in accordance with their professional standards, and internal control to provide performance management services. For example, if there is a recession in Romania, it will increase the risk of non-collection of taxes and duties and consequently we have to cut spending to fit into budgets by the end of the year.

From the above presented, it is clear the broad problem posed by the risk assessment based on their great diversity, their permanent evolution, but especially the implications that the risks inherent in today's management, politics, which are transmitted and have a great effect on individuals, those who are confronted or can even say they are struggling with the "perfection" of the risks. In this extremely tough context, we find that the assessment of the risks respecting the phases they have to go through uses classical risk arguments and

control activities, focusing on the self-control of those involved, setting key controls on the flow of procedures, and, most importantly, constantly adapting control activities to the evolution of risks.

Conclusions

Internal audit is a profession that has been redefined over the years, from the desire to respond to the changing needs of entities. In addition, through their activities, internal audit adds value to organizations in which they are performing. Internal audit can act as an efficient and effective agent of change in economic organizations, as long as it is capable of self-refinement, that is to say it is its own agent of change. In other words, internal audit can help entities progress as long as they themselves adapt their procedures, methods, concepts, and mentality to management requirements and expectations.

Internal audit has become an essential component in the structure of any modern organization. Internal auditing ensures greater efficiency through a more appropriate use of human and material resources, as well as better coordination between the different departments of an entity.

Internal audit contributes to building a reputation for integrity, which in turn will help develop trusted business relationships. Also, internal audit will provide the necessary premises for the organization to play a positive role in the community by providing a public image and strengthening its image of seriousness.

As any activity, in particular, and internal audit (and primarily public internal audit), reveals a series of malfunctions resulting from the content of the normative acts and, on the other hand, the confrontation with the realities of an economy market. The existence of a modern legal framework and of rules and procedures developed in accordance with internationally accepted auditing standards and good practice in the European Union would be fundamental guarantees that public internal audit is a true agent of change within public institutions.

The key to auditing is to recognize that auditing can also be of greater value if it analyzes aspects beyond traditional financial issues and focuses on points of interest for a broader audience (such as the perception of the true image of the financial statements of the economic organization).

Bibliography

Berheci, M. (2010). *Valorificarea raportărilor financiare. Sinteze contabile: teorie, analize, studii de caz.* Bucureşti: Editura C.E.C.C.A.R.

Briciu, S. (2006). *Contabilitatea managerială, aspecte teoretice şi practice*. Bucureşti: Editura Economică.

Cucui, G. (2007). *Sistem informatic pentru managementul financiar-contabil al întreprinderii*. Târgovişte: Editura Bibliotheca.

Cucui, I., Man, M. (2004). *Costurile şi controlul de gestiune*. Bucureşti: Editura Economică.

Cucui, I., Dima, I.C., Petrescu, M. (2007). *Econometrie managerială*. Bucureşti: Editura Universităţii Naţionale de Apărare" Carol I".

Dănescu, T. (2007). *Audit financiar: convergenţe între teorie şi practică.* Bucureşti: Editura Irecson.

Dicţionar de macroeconomie. (2008). Bucureşti: Editura C.H. Beck.

Jinga, C. G. (2009). *Audit financiar*. Bucureşti: Editura A.S.E.

Munteanu, V. (coordonator). (2015). *Audit financiar-contabil. Concepte, metodologie, reglementări, cazuri practice*, Ediţia a III-a revăzută şi adăugită. Bucureşti: Editura Universitară.

Munteanu, V. (2015). *Posibilităţi de pefecţionare a sistemului informational financiar-contabil prin utilizarea indicatorilor de pilotaj şi a tabloului de bord*, Revista *Universul Strategic*, nr.3(23)/ iulie-septembrie 2015

Niculescu M., Vasile N. (2011). *Epistemologie – Perspectivă interdisciplinară*. Târgovişte: Editura Biblioteca.

Popa, Şt., Ionescu, C. (2005). *Audit în medii informatizate*. Bucureşti: Editura EdExpert.

Sandu A. (2012). *Metode de cercetare în ştiinţa comunicării*; suport de curs. Iaşi: Universitatea Mihail Kogălniceanu.

Tanti, C., Morariu, A. (cond.st.). (2012). *Metode şi tehnici de eşantionare utilizate în serviciile de audit financiar contabil* - teza de doctorat, Bucureşti: A.S.E.

Tătaru, V. (2007). *Auditul financiar*. Bucureşti: Editura Cavallioti.

Todea, N. (2009). *Teoria contabilă şi raportarea financiară*. Alba Iulia: Ed. Aeternitas.

Toma, M. (2009). *Iniţiere în auditul situaţiilor financiare ale unei entităţi*. Bucureşti: Editura C.E.C.C.A.R.

Sen, D., Inanga, E. (2009). Creative Accounting In Bangladesh and Global Perspectives. *The Association of Accountancy Bodies in West Africa Journal*, 1.

Vasile, E., Croitoru, I. (2012). **"***The Integrated System for Risk Management - Key Factor in the Management System of the Organization***"**. Croatia: Editura InTech. ISBN: 979-953-307-789-4.

Standardele Internaţionale de Raportare Financiară. (2011). Partea A, "Cadrul General conceptual şi dispoziţii", Bucureşti: Editura CECCAR.

https://global.theiia.org/standards-guidance/mandatory-guidance/Pages/Core-Principles-for-the-Professional-Practice-of-Internal-Auditing.aspx/Romanian

https://global.theiia.org/translations/PublicDocuments/Code%20of%20Ethics%20Romanian.pdf

https://global.theiia.org/translations/PublicDocuments/IPPF-Standards-2017-Romanian.pdf

www.oecd.org

www.theiia.org/itaudit

http://discutii.mfinante.ro/static/10/Mfp/audit/StrategiaAPI2018-2020.pdf