Considerations on Planning Internal Public Audit – Risks Arising from the Use of Technological Tools and Legislative Changes

Costan (Popa) Lavinia
Pascu (Popescu) Gabriela
Bucharest Academy of Economic Studies, Doctoral Accounting School,
lavinia.n.popa@gmail.com
gaby.popescu@yahoo.com

Abstract

The planning of the public internal audit activity includes audit missions on the activities of the public entity as well as on the activities carried out within the subordinated public entities under the coordination or under its authority. In order to ensure the compliance with the applicable legislation, the planning of the public internal audit activity should include missions regarding the information systems and during the internal audit engagements, it will be assessed whether information technology supports the entity's strategies and objectives.

The usage of information technologies within a public entity includes the selection of solutions designed to the activities which are carried out (mobile devices, Cloud technologies, software applications). Effective use of these products through the usage of all the functionalities available and relevant to the entity improves the activities of all structures, including internal audit work.

Key words: public internal audit, mobile devices, Cloud technologies, software applications.
J.E.L. classification: H83, M42, O32

1. Introduction

Planning the activities which are carried out within the organizations are fulfilled in the short, medium and long term. The internal audit activity is planned according to the Standards 2010 - Planning (The Institute of Internal Auditors, 2017), which requires the head of the internal audit department to establish a Multi-annual / Annual plan of activities based on risk analysis. Within the framework of the internal public audit structure, the planning activity is carried out by developing the documents of the Multiannual Internal Audit Plan and the Annual Internal Audit Plan (Ministry of Public Finance, 2013), which is accomplished by selecting the objectives of the internal public audit activity.

2. Theoretical background

In accordance with the legislation in force, the elaboration of the Multiannual / Annual Internal Audit Plan should take into account the following substantiating elements:

- *the risk analysis* based on the activities carried out within the public entity and those prescribed by law to be audited;
- deficiencies previously identified;
- *major legislative changes*;
- following the periodicity in auditing (at least once every 3 years);
- appropriate types of audit;
- the professional training provided by Law no. 672/2002 on public internal audit, republished (minimum 15 days);
- possible ad-hoc missions;
- counseling missions introduced as mandatory;
- reporting and follow-up the recommendations.

The inherent risks may affect the achievement of the specific objectives of the public entity. In this context, it is mandatory that internal auditors should have proper knowledge for identifying, prioritizing and assessing risks (The Institute of Internal Auditors, 2017; The General Secretariat of the Government, 2018). Planning internal audit engagements requires extensive risk analysis. Activities identified with a potential high risk exposure will be included in the Multiannual /Annual Internal Audit Plan, so the auditors will be responsible for verifying the ongoing risk management and internal control measures implemented and designed to keep identified risks at acceptable levels.

The risk profile (Reding, K.F., 2013; Sobel, P.J., 2009) of information technology implementation increases with the emergence of new threats, new threats which are generated by the technological tools used in current activities of the company. In this context, entities address the risks of information technologies by using new risk analysis models/ patterns. This process will begin by identifying, assessing and managing the risks associated with each activity, in order to subsequently determine the risk mitigation measures and the level of responsibility.

The latest Public Sector Audit Report published by the Ministry of Public Finance concludes that during the year 2016, 11.725 internal audit missions were performed, of which 9.756 assurance missions. The insurance missions were allocated to the 8 areas provided by the current legislation: budget, financial-accounting, public procurement, human resources, IT, legal, European funds and special functions. Of the 9.756 missions of insurance, only 5% approached the IT field. Moreover, according to the Report, 62.436 recommendations were followed at the level of the main credit officers, out of which only 1.8% were form IT field.

Analyzing the data presented above, we consider mandatory to have a good understanding of the process of identifying risks related to information technologies and legislative changes when using the methodology of planning the public internal audit activity.

3. Methodology

The methodology for risk assessment of the activities carried out within the public entity which is used by the internal auditors in the planning process of their activities, it provides the elaboration of a Multi-annual audit plan lasting a period of three years. This audit plan is designed to determine whether key controls within the public entity work effectively.

The methodology used to design the plan includes the following:

- conducting interviews with key employees within the public entity's departments /services /offices;
- shaping a risk analysis model;
- developing the audit plan based on information gathered from the risk matrix.

4. Findings

To identify activities involving the use of information technologies/ major legislative changes and the related risks to include them in the Multi-annual /annual internal audit plan we have followed the steps described in the Methodology chapter.

4.1. Interviews with key employees

The first step to identify activities involving the use of information technologies is the key employee interviews for:

- identifying the organizational structure of the entity according to its activities;
- understanding the degree of involvement of the organization's management in the exercise of internal / managerial control activities;
- the assessment of potential risks that may affect the activity of the public entity.

The purpose of the interviews with the management is to identify the areas of activity that they consider to be affected by major risks, including those risks which are generated by the introduction of new information technologies, or where they are experiencing difficulties performance of service duties.

4.2. Risk analysis model for activities involving the use of information technologies

The risk analysis (Ministry of Public Finance, 2002) is done by elaborating two working papers:

- Worksheet no.1 - Identification of the processes / activities / structures / programs carried out within the entity and the related risks;
- Worksheet no.2 - Determination of the total score of the risks and their hierarchy),

and it is completed by hierarchizing the main areas / activities of the public entity according to the associated risk.

The main elements of risk (materiality, exposure to losses, control environment, complexity of operations, quality of management, integrity of the data processing environment, the last audit period, the results of the last audit, legislative impact) are established in order to obtain a score of the risk associated with each activity carried out at the level of the public entity.

4.2.1. Risk analysis model for activities which involve the use of information technologies

Analyzing the computerized environment of public entities from the point of view of internal audit, the top three most relevant types of technologies have been identified in terms of usability. In this context, we consider it important to include in the planning of internal audit missions the activities involving use:

- mobile devices;
- Cloud technologies;
- dedicated software applications.

4.2.1.1. Mobile devices (laptop, tablet, phone) are widely used and it allows employees to access and share information from anywhere, at any time. Increasing the capacity of mobile devices and adapting them to the needs of employees, these devices have been transformed from simple ways of communicating into an integral part of how people perform their tasks.

The main risks that can be generated by the use of mobile devices are:

- the loss or leak of important information;
- device security vulnerabilities, operating system, or anti-virus limitations;
- theft / loss of the device;
- using the device both professionally and personally.

Internal audit should include at least one privacy policy assessment, mobile configuration and device configuration settings checking, event management practices for lost / stolen devices, or mobile device vulnerabilities generated by accessing a communications network.

The public entity's strategy regarding the usage of mobile devices must be known throughout the entire organization. Internal auditors support the public entity in achieving its objectives, including through support to audited structures in the identification and management of key risk hazards. However, it is noted that the strategy of public entities on mobile devices has to evolve, and the implication of internal auditing in this area can add value to the organization.

4.2.1.2. Organizations have started to use **Cloud technologies** because it noticed more and more advantages such as: increasing the efficiency of IT products, reducing operating costs, providing operational flexibility and generating a competitive edge.

The main risks that the usage of Cloud technologies may generate are:

- a generic version of applications because most of the users are experiencing challenges when it comes about the implementation and usage;
- the continuous development of Cloud technologies generates the risk that the entity system will no longer work according to supplier's product;
- legality and national regulations on how information is handled in the Cloud;
- information security (privacy, integrity and access to data).

The strategy of the public entity needs to be redefined according to the usage of Cloud technologies. In this context, internal auditors assess whether policies have been well developed and proper internal controls were implemented and aligned with the general objectives of the public entity. It will also assess the organization's preparedness level for implementing Cloud technologies.

The internal audit engagement may include assessing information security practices and procedures, contract clauses, and internal security measures that it have been taken in order to protect public entity data or secure authentication protocols for users working in the Cloud.

4.2.1.3. Software applications dedicated to some activities are also implemented within public entities. Most public entities chose to purchase dedicated software to deliver the expected benefits, to the detriment of internally developed software.

The public entities have increased significantly their investments in the training and retraining courses offered to their employees to improve their knowledge and capabilities in the use of programs. Choosing a dedicated software application typically has three basic features:

- maturity of the program;
- program execution;
- market competitiveness.

The installation of dedicated software applications may generate the main risks as following:

- high risk activities that it can't be prioritized to provide management with confirmation that they have been independently verified;
- the governance processes implemented partly ensure alignment with the company strategy;
- the implemented processes and controls are not optimized to use available technology;
- lack of documented control flow for implementation of the application;
- the benefits obtained with the implementation of the application are partly in line with the planned/ expected benefits.

The efficiency of the internal audit is found in confirming that the installed application manages the processes in the entity properly and the procedures and controls are properly implemented.

4.3. Risk analysis model for major legislative changes

As far as the changes to the 2018 legislative framework are concerned, the internal auditors showed a real interest in the General Data Protection Regulation (GDPR) legislation, which entered into force on 25 May 2018. In electronic or paper form, data protection has also become an element essentially within any organization. In the case of public entities, the processes / activities / actions on which the GDPR has its effect need to be included in the Multiannual / Annual Internal Audit Plan.

The main risks that can be analyzed with the GDPR implementation audit are:

- the lack of a person in charge of the privacy policy within the entity (compliance /security team or data protection officer);
- the lack of a system or operational procedure regarding the confidentiality of data within the system of internal managerial control;
- the procedure was not broadcast or the access for employees and third parties was not provided;
- partial identification of activities involving the processing of personal data;
- failure to implement the process of identifying and managing information security incidents (the lack of an information security management system that includes privacy of personal data).

5. Conclusions

The internal audit department is uniquely positioned to the other structures of a company to help stimulate organization development and create value by reviewing activities. Spencer Pickett (2012) believes that the purpose of internal audit is to support the organization's management because it is interacting with increasingly complex systems that are evolving in a very short time.

Concentrating internal audit on risk management activities in areas with the highest impact can improve the image of internal audit within the organization and can benefit from increased management confidence.

High risk areas are constantly changing and developing, but internal auditors usually focusing on *information technologies* and the *legal framework* for doing business.
Improving activities by properly managing the risks of information technologies/ legal framework can create added value. The information technologies used in public entities are constantly developing and offer the expected benefits in some areas. Moreover, with the widespread use of information technologies presented above, new opportunities can also emerge for the development of integrated audits.

The public internal audit activity has gained, in the last few years, a special consideration from the management of the organizations, by increasing the level of trust generated by risk reporting to stakeholders. Technological progress can streamline most of the work done within a public entity, including internal audit work, if a pertinent risk analysis is carried out. Identifying types of ideal technologies that fit for the entire public entity would create an opportunity for the convergence of solutions.

6. References

- Ministry of Public Finance, 2002. *Law no. 672/2002 on Public Internal Audit, republished*, [online]. Available at: http://www.dreptonline.ro/legislatie/legea_auditului_intern.php, [Accessed on 05.12.2018].
- Ministry of Public Finance, 2013. *Government Decision no. 1086/2013 for the approval of General norms regarding the exercise of the public audit activity*, [online]. Available at: https://codfiscal.net/40052/hg-10862013-normele-generale-privindexercitarea-activitatii-de-audit-public-intern, [Accessed on 05.12.2018].
- Ministry of Public Finance, 2017. *Report on the internal audit activity of the public sector in Romania for the year 2016*, [online]. Available at: http://discutii.mfinante.ro/static/10/Mfp/audit/Rap_activ_audit_intern_sect_public_2016.pdf, [Accessed on 05.12.2018].
- Reding, K.F., 2013. *Internal Auditing*, Third Edition, The IIA Research Foundation.
- The General Secretariat of the Government, 2018, *Order no. 600/2018 regarding the approval of the Code of internal / managerial control of public entities*, [online]. Available at: https://sgg.gov.ro/new/wp-content/uploads/2016/04/0387.pdf, [Accessed on 05.12.2018].
- The Institute of Internal Auditors, 2017. *International Standards for the Professional Practice of Internal Auditing*, [online]. Available at: https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards.aspx, [Accessed on 05.12.2018].
- Sobel, P.J., 2009. *Auditor's Risk Management Guide (Integrating Auditing and ERM)*, Publisher CCH.
- Spencer Pickett, K.H., 2012. *The Internal Auditing Handbook*, , New York: Publisher John Wiley şi Sons Inc, DOI: 10.1002/9781119201717.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1544526372979&uri=CELEX:32016R0679, [Accessed on 05.12.2018].