DE GRUYTER OPEN
International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXIII No 2 2017

THEORETICAL ASPECTS REGARDING INFORMATION SYSTEMS AUDITING WITHIN THE MILITARY ORGANIZATION

Marius MILANDRU, Daniel Sorin CONSTANTIN

"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
mnmilandru@yahoo.com

Abstract: *As part of the general effort to modernize the financial-economic system, in both private and public sectors, the concept of internal auditing is fairly recent. The development of information technology has significantly contributed to the integration of information systems into management related activities (economy, logistics, finance and accountancy, etc.). The integration of new information technology into the practice of processing, transferring and storing information has brought about a series of threats and vulnerabilities of the information system. Thus, auditing information systems has become a vital element for all domains and activities of organizations, including the military one.*

Keywords: information system, auditing, risks, vulnerabilities, objectives.

Introduction

The rapid development of automatic data processing systems determined by the emergence and evolution of computer technology and specialized software has had a great impact on the way we store information and monitor the activity carried out by various entities, including the military organization. The technological evolution of increasingly efficient and less costly, highly accessible personal computers has lead to the rapid development of specialized software applications (accountancy and salary calculation programs, records of volume and value, human resources, major staff, etc.), used extensively, even by personnel not specialized in information technology.

The use of new information technology in data processing, transfer and storage has generated a series of *threats and vulnerabilities of the information system.*

Concurrently, the employment of the World Wide Web and the Internet by entities has had a particular impact on the objectives of information system monitoring. Such a development has amplified the risk of using information systems in the remote processing and transfer of data.

Fraud and loss of data in information systems connected to the Internet has reached alarming levels and it has confirmed the necessity to generate within each particular entity *an internal monitoring process that targets the information system.* Thus, managers have tackled the problem of ensuring an accurate and secure environment for the operations carried out in the information system and of correlating these with the objectives and strategies of the organization. In order to neutralize the possible negative effects, the elaboration of a *monitoring procedure* has been established for information systems in all entities. The aim of all these internal monitoring objectives and procedures is to *ensure the security of information systems and to reduce the possible risks related to their operation, posed by any threat and vulnerability of the system.*

DOI: 10.1515/kbo-2017-0094

The intervention of internal auditing within this segment aims to assess the monitoring system, and implicitly, to issue recommendations regarding its improvement, especially in the case of the information system used in the military, as part of the public sector.

2. The concept of information system auditing

The two terms we encounter in common usage as well as specialized literature in Romania are *organizational information system auditing* (sistem informational) and *computer information system auditing* or *IT auditing* (sistem informatic). The contrast between the two terms is rendered by the content and the level of the auditing activity, on the one hand, and the conceptual difference on the other.

Conceptually, *organizational information system auditing* is more inclusive, its objectives covering all levels of the system from the assessment of system design and use to the evaluation of security policies and procedures of the operational and strategic levels. *Computer information system auditing* is a term covering the more specific activity of monitoring the computer system. Concretely, organizational information system auditing includes computer information system auditing. Since in most entities the computer information system constitutes all of the organizational information system, the most widely used term is that of *information system auditing* and the term used for the auditor is *information system auditor.*

Information system auditing is the activity of collecting and assessing evidence in order to determine if the information system is secure, able to maintain the integrity of the processed and stored data, allows the achievement of the strategic objectives of the enterprise and employs efficiently the available information resources. Usually, this activity should be carried out by personnel qualified and specialized in the field of monitoring, security and management of the information systems. The CISA *(Certified Information Systems Auditor)* certificate issued by the *ISACA (Information Systems Audit and Control Association)* represents a professional certification in this field. Although there is a rather close methodological connection between finance and accountancy auditing and information system auditing, the latter is based upon at least four domains: traditional auditing, information systems for management, behavioral science (psychology) and computer science.

Information system auditing can be organized both on the level of entities, within the appointment for internal auditing, and as external auditing performed by people outside the entity.

During an information system auditing the most frequent operations are the assessments, evaluations and testing of the information devices:

- identification and evaluation of risk in the system;
- evaluation and testing of the monitoring within the system;
- assessment and evaluation of the physical information environment;
-assessment and evaluation of the administration of the information system;
- assessment and evaluation of information applications;
-assessment and evaluation of computer network security;
- assessment and evaluation of recovery plans and procedures in case of disasters and procedures to resume activity;
- testing the integrity of the data.

The risks within the information system of the entity must be evaluated as correctly as possible by both managers and auditors.

Generally, in order to identify and evaluate risks, the following measures are taken:

- identification of risk factors;
- ranking of risk factors according to their importance for the audited system;
- determining the frequency and length of occurrence of each risk factor;

- quantification and evaluation of the level of the risk;
- scheduling the auditing activity and allocation of auditing resources according to the established risk level.

There are a series of techniques used to evaluate and quantify risks. One of the most widely known and used is the *score technique,* which is one of the quantitative evaluation methods for potential risks. According to this technique, each risk factor (threats or vulnerabilities) is allotted a weighting (a factor that indicates the importance for each function of the entity) and a risk level.

The result of the multiplication of the *weighting* with the *risk level* determines the *risk of the function,* and, by adding up the individual risks multiplied with their weighting, we determine the *system risk.*

A further method to evaluate risks is to rely on the free judgment of the auditor, who relies on his own experience and the evidence collected on the audited system. In practice, it is recommended to combine the two methods.

Quantifying and evaluating risks in the information system auditing process results in:

- effective determination of auditing objectives;
- efficient allocation of resources for auditing.

Throughout the entire auditing process, the auditor should employ a variety of techniques and procedures to evaluate risks, to evaluate and test internal monitoring, to collect logs, to administer conformity and integrity tests, to assess evidence, to elaborate and transmit the report and follow up on the implementation of recommendations.

In practice, the techniques used by the information system auditor are the following:

- techniques of investigating the audited system;
- techniques of identification and evaluation of risks;
- techniques of testing the monitoring process within the audited system.

The most frequently used techniques for collecting the evidence are the interview, the questionnaire and the flowchart.

The *interview* consists of a list of questions elaborated in order to be addressed to the personnel within the audited system (managers, users, system administrators, etc.). It is a process with a precise purpose implying the formulation of questions in order to obtain answers. The questions should target the aim of the auditing activity, so that the highest amount of relevant evidence can be collected.

During the information system auditing mission, the auditor can interview:

- the managers of the functions that the auditing covers in order to determine the structure and complexity of the audited system;
- the users of the information system applications in order to determine their perception of the utility and errors of the applications;
- analysts and programmers within the system in order to better understand the implemented functions and monitoring process in the applications that these types of personnel create;
- internal auditors or personnel involved in internal auditing in order to determine the level and the state of the monitoring process.

The *questionnaire* is a form of the interview, without the interviewer, in which a series of options are provided as possible answers to the questions so that the interviewee can select or complete the answer on his/her own. The structure of the questionnaire should be planned in such a way that it can evaluate several aspects regarding the risks and the monitoring of the audited system.

The *flowchart* is a graphic representation with standard symbols of the circulation and flow of information and data within the audited system. The auditor can use the existing flowcharts or build them in order to

identify and evaluate strong and weak spots of the monitoring process within the auditing system.
In an auditing mission the flowcharts can be used to:
- identify documents and their circulation in the audited system;
- determine the way in which the data circulates and is processed within the information system;
- identify the addressees of the reports and data files;
- evaluate the quality of the documentation within the system;
- evaluate the monitoring of documents.

3. Specific aspects of information system auditing

The range and ramifications of the use of informatics nowadays have lead to the necessity to evaluate and analyze the information system. The methodological frame associated to an internal public auditing mission aims to obtain an understanding of the requirements of the organization, the identification of existing vulnerabilities, the evaluation of the conformity of the internal auditing by identifying the risks and by applying the recommendations for performance improvement. The identification of the specific risks in the information system requires an analysis of the weaknesses in the monitoring process and the vulnerabilities of the system in order to assess the present or possible impact.
Examination of the integrity of data is a stage that precedes the accomplishment of the internal auditing mission as the auditors have to make sure that that the results of the final reports are based on complete, precise and reliable data.
The main criteria to be observed during a system auditing mission in the field of informatics are the following:
-the available resources, equipment (processors and peripherals) and associated operation resources, their efficient, effective and economical use. It is essential, for an effective evaluation, to clearly delimitate the responsibility for acquisition from that of inventory;
- the activity of the auditor which should be focused on the performance monitoring of the use of information system resources and the implications it can have on the inventory of the entity.
The auditor should be an information system specialist, even though, he has to be familiar with the terminology and have some specific knowledge. It needs to be emphasized that throughout the evaluation certain important aspects may be revealed that require an elaborate inspection by a specialist. Thus, the auditor will focus on assessing whether the necessary information system resources are allotted in order to cover the inventory of the entity and if this is accomplished at a reasonable price.
From the point of view of the type of evaluation, the activities related to the information system are divided into:
-activities related to planning and performance;
- activities related to operation.
The activities related to planning and performances occur based on a cycle that includes:
- a general study of the field in which the information system is used within the entity, through which a development plan is elaborated for the information system, also known as system plan or plan of mechanization, containing the applications that are to be developed and the priorities;
- a detailed planning of the concrete applications which are intended to be initiated.
This process starts with the technical and economical evaluation of the application, followed by a logistic planning of its course which is described in a work plan based on which the progress of the application is monitored. The work plan should be carefully assessed by the auditor as it provides the efficient and the economical use of the resources implied, in one word, it reveals the efficiency of the application.

In the assessment of this plan the following aspects should be observed:
-the participation of the users, which has to be sufficient in order to make sure that the application covers needs and expectations, that the samples are satisfactory, and, that the logistics related to the conversion of the present system into a new one is well planned and monitored;
- the training of the users for the operation of the application, including manuals and necessary instructions;
- the necessary modifications in the case of accountancy and administrative procedures that occur due to the use of the new application, as well as the timely availability of materials, forms and registers associated with these procedures;
- the selection of criteria related to the completion of the application where we should mention the use of program packages vs. programming, the use of a data base structure vs. specific archives, decentralized processing vs. centralized processing, methods of data transfer (communication lines vs. physical media), immediate processing (on line) vs. differentiated (batch). The criteria of completion influence efficiency, effectiveness and economy as well as the monitoring and reliability of the processed information;
- the fragmentation of the work plan into partial modules with concrete results and terms of execution. This will allow a better surveillance and monitoring of the development process and it will provide partial results for the whole length of the process;
- the sufficient time allotted in the work plan to document the application (functionally and technically). This aspect is important from the point of view of efficiency and effectiveness (in employment, maintenance, and modification of the application) as well as that of internal control;
- control mechanisms regarding the execution of the work plan, starting with organizational aspects (such as an assessment committee that monitors the participation of users) and ending with highlighting the progress achieved (such as recurrent reports on the level of achievement and the documentation of the decisions taken – modifications, deadlines, priorities, conceptual changes).
The operation activities occur chronologically through a cycle that contains the feeding of data which is to be processed, processing operations and the obtaining of results. Depending on the characteristics of the application, these phases can succeed without interruption or can take place punctually, independently, or in a combined form. There are special methods, typical of information technology, to limit and monitor access to equipment and data on magnetic media, as providing a personal password for the various access and confidentiality levels and automatic registration methods to use of equipment.

4. Conclusions

The contemporary complexity of the financial and economic activities emphasizes the necessity to use accountancy and auditing techniques and tools that correspond to the requirements of information system users.
Such a performance cannot be achieved through only classical auditing techniques; therefore, their completion with computer assisted methods is a natural and beneficial development for the aims of internal auditing. The methodological framework around a public internal auditing mission aims to obtain an understanding of the requirements of the organization, the identification of the existing monitoring procedures, the assessment of the conformity of internal monitoring through the identification of risks and the recommendations for its improvement. The identification of significant risks for the information system requires an analysis of weaknesses in the system and the monitoring process, in view of assessing the

present and the potential impact. The inspection of data integrity is a phase that precedes the accomplishment of the auditing mission as the auditors need to determine that the results of the final reports are based on complete, precise and reliable data. Cases of fraud and error committed with the help of the computer are not uncommon. Generally, information system auditing aims to complete an analysis on both general and particular levels, which sometimes affects the activities related to the information system, influencing the monitoring of the applications that exist in the system.

References

[1] Arsac, J. *Informatics, Romanian Encyclopedic Publisher,* Bucharest, *(1973).*

[2] Boulescu, M., Fusaru, D., Zenovic, G., *The Auditing of Information Systems in the Field of Finance and Accountancy*, Bucharest, Economic Publisher, *(2005).*

[3] Popa, Ş., Ionescu, C., *Auditing in the Field of Information Systems*, Bucharest, 2005.

[4] Zaharia M., Cârstea C., Sălăgean L., *Artificial inteligence and expert systems in assisting economical decisions,* Bucharest, Economic Publisher, (2003).

[5] Whittington, O., Kurt, P., Walter, B., Principles *of Auditing. Tenth Edition*, Boston, 2006.