The Audit of Accounting Information System Infrastructure

Mihalache D. Arsenie-Samoil
"Alexandru Ioan Cuza" University of Iași, Doctoral School of Economics
arsenie_samoil@yahoo.com

Abstract

The phenomena that mark the economic environment in recent decades are under the sign of globalization, interdependence and interaction. Whatever happens in any corner of the world, affects more or less extensively the local economic environments. In these circumstances, any organization, regardless of its activity profile, size and space in which it operates, must prove its viability, ability to communicate and adapt in order to achieve economic and financial performance to make it increasingly competitive.

This paper aims to address the issue of accounting information system infrastructure audit, in terms of globalization, an activity which involves evaluating all aspects of automated data processing systems, including related manual processing activities. Key concepts relative to what is the audit of accounting information system infrastructure, audit aim, audit methodology (7 steps), audit report, as well as steps to be followed in implementing post audit corrections, are highlighted.

Key words: infrastructure, accounting information system (AIS), audit.

J.E.L. classification: M4, C4, D8, L14, E42, G32, H83, L86, Q56.

1. Introduction

Accounting is the most important subsystem of an organization’s information system. Also, accounting is the main source of information in an organization. Economic data provide about 80% of the total circulating information throughout an organization. Of these, about 46-50% are information provided by accounting [1].

This way of seeing the organization makes accounting information system the most important element of an organization’s information system for the following reasons: accounting information system is the only provider, to management and external users, of an overview of the entire organization, accounting information system interlinks other important information related subsystems such as marketing, personnel, research and development, production, etc., in such a way that information in all these subsystems is eventually expressed in financial terms, non-financial information in areas such as social responsibility and human resources are integrated with accounting information to enable decision making, accounting integration with other subsystems leads to higher speed and increased accuracy in providing information to users.

From the perspective of the development of information technology and communications (IT&C), accounting is subject to many challenges: the increasing number and importance of external events for any organization, changing the means of producing economic events, the latter become increasingly means of electronic nature, the existence of information technology capable of automating specific accounting operations: identification, measurement, recording and reporting; globalization and developing information technologies ensure that organizations are no longer monolithic structures, but they tend to become increasingly complex structures, interdependent and interoperable with other agencies and organizations; internal and external users request more and more information, more diverse, more complex and in increasingly shorter intervals of time.

From this perspective, an organisation’s accounting information system infrastructure (AISI) includes: equipment (hardware resources) – the hardware of the system, network components – communication network infrastructure; classifications – databases – data infrastructure; software package (the program-products) the system
software infrastructure; processes – the logical infrastructure of the system; employees – the social infrastructure of the system; the implementation strategy.

A principle widely accepted by management says an activity can not be operated and managed if it can not be measured. The IT&C audit provides the measure of using the accounting information system infrastructure in an organization [3].

The audit of accounting information system infrastructure is a thorough analysis of the information system in an organization. It is a very important tool for the organization's management when evaluating the efficiency and effectiveness of using IT&C resources (hardware and software).

IT&C technologies are under steady development, so that both security systems and modes of attack are analyzed and perfected every day. The only way an organization can protect itself by implementing the best practices in the field is an audit of information system infrastructure.

IT&C audit should be conducted by a specialized, independent company and in no case can be made by its service provider in information system implementation.

The audit of information system infrastructure is a kind of "insurance" that things are on track and that any difference will be analyzed and eliminated as the company's accounting information system is in compliance with safety and quality standards stipulated by law and are consistent the direction in which the organization operates.

It is generally accepted that the audit of information system infrastructure is the only and best way for company management to ensure that security technologies and practices used are performing in accordance with specifications set [5].

The audit of accounting information system infrastructure is the collection and evaluation of evidence in order to determine if the computer system is secure, maintains the integrity of data processed and stored, enables the achievement of company's strategic goals and uses information resources effectively.

In an audit of accounting information system infrastructure, the most common procedures are checking, assessing and testing information resources, such as:

- identifying and assessing risks in the system,
- evaluation and testing of system control,
- physical examination and assessment of information environment,
- checking and evaluation information system management,
- checking and evaluation of computer applications,
- checking and evaluation of computer network security,
- checking and evaluation of plans and procedures for recovery from hazardous situations and business continuity,
- testing data integrity.

The audit of the accounting information system infrastructure AISI is an essential method by which an information system IS is checked as to whether it has achieved the goal for which it was designed. The standards clearly define the scope, tasks, milestones, content auditing and forms completion. The AISI audit is an area that includes all auditing activities for the following:

- specification, design, software, databases,
- processes typical of a program life cycle,
- a computer application,
- a management information system and the maximum complexity of a portal associated with a virtual organization.

The AISI audit may relate to the risk assessment of physical security information, logic security, management of changes, assistance plan, etc. In general, the information audit refers to a set of computer processes in order to meet the specific customer requirements.

From another point of view, the AISI audit is the mechanism for examining the efficiency of organizations, systems, risk processes and controls. The audit enables management to: discover what actually happened at a given moment in time, detect potential problems before they are too late to remedy, assess the business situation objectively, accept reality and, knowingly, make decisions even if they are difficult, implement corrective actions, changes and improvements where necessary.

The AISI audit is not just about compliance. The audit may include an element of control on the compliance with policy/standards/internal company procedures or laws, rules and external terms of trade, but compliance is a daily activity of management. Experienced auditors control whether management processes to achieve and assess compliance are effective, which
rules are adequate and sufficient for the audited IS. More often, auditors will find out the absence of compliance and are less inclined to look for symptoms of problems in depth.

Accounting information system infrastructure audit is the process of collecting and evaluating evidence to determine if the accounting information system and resources involved are adequately protected, maintains data integrity, provides relevant information and contributes to achieving organizational objectives.

2. Purpose

The AISI audit, used by an economic body in its economic activities, aims: to ensure the precision, completeness and accuracy of data input, as it affects the results of processing performed; ensuring processing accuracy of data input the system, meaning that their results observe management rules specific to that economic organization and current legislation; ensuring accuracy and integrity of the system output, that it is exactly the one required by the managers and financial control bodies of that economic agent; ensuring fairness of control procedures (controls) used for auditing the respective information system

The accounting information system infrastructure audit within the organization requires, as a whole, a high level of analysis; in particular, the integration of applications, systems, infrastructure and how they affect the entire organization's information system will be analysed; identifying and eliminating weaknesses in information system; minimizing the risk to which the organization is exposed; raising awareness of potential risks involving the current computer system in project development and critical points where intervention is necessary to remove these risks; safe use of updated, developed technology by applying security policies that comply with the specific organization.

The AISI audit process helps companies cut costs by finding more efficient ways of protecting hardware and software and provides a better management relative to the application and use of security technologies and of processes.

As a result of this audit, a set of suggestions for changes to be made in the present computer system structure will be provided.

3. Methodology

In order to achieve the AISI audit, the definition of the overall audit plan and audit program is considered. The structure of the plan and program definition are standard, assuming completion of the mandatory steps. The specificity of the software, computer application or computer system and their complexity, entail some breakdowns that differ from one general plan to another, namely from one information audit program to another. The tasks to be included in the plan, the phasing in the program stages, involve elements of variability strictly related with the structure and diversity of software products analysed [5].

The information analyst has available a number of techniques and methods that can be adapted to the context. A statistical calculation or optimization computer program and an application using a database will be analysed in different ways. For a complex information system, there are adequate methods of auditing, while in auditing web applications emphasis is placed on target group satisfaction. The audit for mobile applications is based on ensuring continuity, compatibility, fast access to resources, and especially on the level achieved in securing the data flow in the whole system.

Therefore, in the AISI audit process, planning and defining the audit method is essential. Choosing an inadequate method leads to the use of inadequate tools and the audit results are speculative [9].

The choice of method relies on obtaining information on the context in which processes take place in relation with the software product, the computer system or computer application, as objects of auditing.

The audit report is based on questioning the IT&C staff in order to evaluate and monitor policies and current documents, perform risk analysis that relative to workstations, servers and the whole network and evaluate network services and configuration files. The assessment will highlight potential errors and/or security
holes present in the computer system.

STEP 1 includes the following stages: 1. Meetings, interviews and/or direct observation of staff in the company; 2. Collection, compilation and review of current documentation, checking licenses of installed software. Analysis of all IT policies underlying the whole system operation (policies on the terms of use of IT infrastructure, policy on Internet, e-mail use, backup policy, passwords, access to resources, etc.); 3. The analysis of electronic document flow within the company, as well as outside the network with external partners (customers and suppliers);

STEP 2 includes the following stages: 4. The analysis of IT&C requirements in the company; 5. Evaluation of the human factor in the IT department. Classification of IT staff according to qualifications and professional skills; 6. Evaluating performance in the IT department based on measuring the time in which it responds and resolves any incidents;

STEP 3 includes the following stages: 7. Evaluation and verification of hardware infrastructure (workstations); 8. Evaluation and verification of software infrastructure (installed applications, licenses); 9. Evaluation and verification of the servers in terms of hardware, software and traffic;

STEP 4 includes the following stages: 10. IT&C analysis in terms of security; 11. Analysis of connectivity between locations and with the outside (location, Internet connections, VPN channel, remote access); 12. Analysis of network topology in locations;

STEP 5 includes the following stages: 13. Assessment of IT&C staff based on know-how (knowledge of processes); the possibility of training some of the IT staff; 14. Verification of IT applications used widely within the company;

STEP 6 comprises the following stages: 15. Testing of the backup/restore procedure; 16. Analysis of disaster recovery plan;

STEP 7 comprises the following stages: 17. Analysis of acquisition services; 18. Analysis of IT&C technologies used in business activity;

4. Audit Report

The audit process is completed with a report containing proposals for measures to reduce and keep major AISI risk under control. Audit report is a work of synthesis which is based on a series of checks on interconditioning between modules, programs, i.e., between the subsystems of the information system.

The audit report is an essential element of auditing through which the situation of the audited system is shown as it was evaluated by auditors [3]. The audit report communicates the auditors' findings and conclusions to the audited party. The objectives of the audit report are: restore managers' confidence in the information system, immediately after the auditing has finished; to provide useful advice on improving inspection procedures and efficiency of operational activities; to provide an official record of the audit activity and managers' response.

The audit report is a structured text which includes: the presentation of context; the result of the audit process; final evaluations; records of each stage of the audit process.

The audit report will consist of two parts: the AISI evaluation results at present; the auditor's recommendations following the analysis made in the evaluation stage. Finally, the audit report will result in a set of documents presenting an objective evaluation of the IT system, which enables the implementation of all necessary measures to correct and remove potential errors.

5. Implementing corrections

The most important result of the process of accounting information system infrastructure audit is the list of weaknesses discovered. Being aware of the specific weaknesses faced by the organization is a good step towards developing a comprehensive program to remove these shortcomings, thus avoiding the occurrence of malfunctions in the day to day activity [8].

The process of implementing corrections (post audit) involves the following stages:
Establish priorities. Following the audit report, we receive a lot of information with variable degrees of importance. Each of these pieces of information will be assigned a risk level. The most critical points will relate to the most critical systems which can be caused by public access to the network or events that involve the transfer of critical data.

Assign roles. It is very important to decide who will manage each task. At this stage, we must ensure the necessary resources, such as budget and/or time have been allocated for each employee to perform each project.

Requesting reports. After roles have been assigned to each individual involved in the correction of weaknesses following the audit, we must ensure that the project will be completed as promised, within a certain deadline. A status report has to be presented regularly, so as to provide for any delays or problems that may arise.

Individual evaluations. Once the correction of security "holes" or equipment reconfiguration have begun, we can start testing the corrections that were made. Before scheduling and requiring a second audit, we must ensure that the weaknesses detected in the first audit were corrected. This approach will help us develop a plan for continuous improvement in the organization. If status reports can be submitted to the management and with an ongoing dialogue on the status of projects, it can be shown that we are on "top" of any problems and it is justified to ask for continuous support to audit processes and correction making.

Schedule next IT audit. It is a rare situation for an organization to return to conduct a new audit, the second, even if the first one has failed. However, companies should have regular assessments of the AISI audit. The scope and frequency “will depend on who we are and what we do." Ideally, it is recommended for an organization to conduct an AISI audit every 6 months.

Since the accounting information systems are constantly developing and upgrading, the AISI audit process can be seen as a regular process.

This is because once a problem has been fixed, another problem may occur, but as long as we perform regular audit assessments, we can continuously improve accounting information systems.

Therefore we believe that the analysis of information system should be a continuous one [11].

6. Conclusions

AISI audit represents a distinct branch of the audit. It includes techniques and methods of auditing software, computer applications, traditional information systems, modern computer systems, mobile applications, as well as all applications using Internet resources.

With globalization and integration, as complexity of processes in the information society increases – a society of knowledge, the requirements of information systems impose a very high level of credibility which only information audit is able to support.

The achievement of AISI audit contributes to: the improvement of information systems and process controls; prevention and detection of errors and fraud; reduction of risk and improvement of system security; planning for recovery in case of accidents and disasters; information management and system development; assessment of efficiency in the use of resources.

The information systems auditor must be able to assist the management team in determining the size of the accounting information system infrastructure and the necessary number of staff, the business areas where computer systems are used effectively, the nature of business, potential loss if the computer system crashes, the extent of manual controls and the degree of technical complexity.

In order to achieve an effective auditing process, it is necessary to go through the following steps: defining the object of accounting information system infrastructure audit; building the audit plan; assignment of tasks to each member of the team of auditors; taking the structures of tables for recording the results of auditing; performance, step by step, of the auditing process using established standards, techniques and methods; recording the results of and evaluating each step taken; re-grouping of documents from various
stages of the auditing process and building of the final report.

There are two results for a product subject to AISI audit.

The first case, the negative one, corresponds to the situation where the audit process leads to the conclusion that there are key differences between the actual accounting information system and the accounting information system expected by the user; the system does not perform the established accounting information processing functions fully; reports obtained are only a part of the established ones – the auditors recommend adding new modules to develop planned, but unrealized, processing; variances are caused by incomplete results within the report - we recommend adding modules that bring reports to the level of completeness required; the differences relate to the way indicators are calculated – we recommend changes in program sequences that either contain all the information for processing or change filtering criteria or modify assessment expressions; if cases are identified on the upper levels of the tree associated with accounting information system, the requirements for change stipulated in the audit report have a larger scope. After having made the changes in the hardware infrastructure, software infrastructure or databases, the audit process is resumed and the findings report turns into an audit report, followed by the issue of a certificate by the auditor, which recognizes the qualities of the computer system and users can rely on the computer system audited.

In the second case, the favorable one, the difference between what is expected by the user and what has been achieved is insignificant or is favorable to the increase in product quality.

Corresponding to the two cases above, the auditor's audit opinion will be one of three types: negative audit opinion when, at the end of the audit, there is one or more noncompliances; qualified audit opinion (with reservations) when there is one or more observations at the end of the audit; audit opinion – when, the end of the audit period, there is no persisting comment or noncompliance.

AISI auditing is meant to transfer confidence and trust in the information system established through a positive result established by a team of auditors, belonging to a consulting firm whose authority has been provided by previous audits.

7. Acknowledgment

This work was supported by the European Social Fund in Romania, under the responsibility of the Managing Authority for the Sectorial Operational Programme for Human Resources Development 2007-2013 [grant POSDRU/88/1.5/S/47646].

8. References