AUDIT INFORMATION CONTENT

Ioan Rus[1]

ABSTRACT: The audit of computer systems shows at least two features that make the audit work not includable in other audit processes such as internal audit and financial audit. These two particularities refer to the specific software used in information systems auditing and real levels of information systems audit. This paper presents the specific levels of a system of auditing and specific techniques available for their implementation in practice. In the end the author suggests proposals for improving specific audit performances in the area of informatics systems.

Key words: Internal audit, Information audit, specific levels of the information audit, operation systems, data centres, data bases, standards for the information audit, CISA® certifications, CISM® certifications.

JEL Codes: C810, C820, K400, D800, M420, L860, O510

Introduction

Information Audit is a particular form of audit which verifies if an Information System achieves the purpose for which it has been developed. The Information System Auditor is represented by a computer scientist specialized in economic informatics and in the finance-accounting field. He is certified as a computer auditor (Certified Information Systems Auditor, CISA) by ISACA ((https://www.isaca.org/CERTIFICATION /Pages/default.aspx) in accordance with conditions set by the Chamber of Financial Auditors of Romania. Globally, the Information Systems Audit and Control Association®, - ISACA is the best known authority in auditing, control and security management systems (Renard , 2003). Regardless of the ideas and trends existing in the literature (Eden and Stanciu, 2004), we conclude that in practice the auditing of computer systems is formal, made within irrelevant levels and with inappropriate tools. The description of the process of audit information, of computer components that need to be audited, of the techniques specific to audit information and their respective resources, represent the main objectives of this work (Dănescu, 2007).

Research activity

The overall objective of the research is to describe and analyze the content, components and computer audit activities. We sought to describe the activities of audit information, to present the role of auditing and how audit information of each specific activity, to illustrate how to audit a information system component using appropriate software programs and to identify specific audit information. We also sought to demonstrate that the methods and tools specific audit information.

Research aims to identify issues audit information and verify the hypothesis that audit information is a specific audit. Audit information can't be included and performed with technical means of other types of audit. To verify this hypothesis the research I did so: we defined information content of audit work, we described the activities and processes to be audited, we described how to do audit these processes and practically exemplified auditing a computer system using Windows operation system from a computer network.

I made a presentation of views in the literature in the field. In particular we sought ideas American professor Chris Davis and his collaborators on the definition and practical issues related theoretical IT audit (Davis, Schiller, et al., 2011). In contrast to these descriptions we analyzed the

[1] "Petru Maior" University, Târgu Mureş, Romania, *e-mail: irus@artelecom.net*

ideas of his "Theory and Practice of Internal Auditing" of specialist Jacques Renard, conducted by the Ministry of Finance in Romania (Renard, 2003). Research findings are included in the following paragraphs of this study.

Description of current state of knowledge

The internal audit is regulated by Law 672/2002 concerning public internal audit and Law 31/1990 regarding trading companies, the internal audit domain includes also information systems. Law 31/1990 regulations do not include provisions regarding information systems audit. Out of the corroboration of these two regulations there can be understood, by means of deduction, that the obligations relative to the internal audit must be accomplished according to Law 672/2002 provisions; these ones regulated the auditing activity as specific law. None of the laws do not make mention of the obligations and responsibilities of the Information Systems Audit and Control Association® - ISACA®, the Romanian filial. Moreover, the legal provisions are not compulsory for private organizations; for public organizations they have working environments within which they can be hardly of formally applied (Rus, Dănescu, 2010).

The audit process of IT systems

I am identified three elements of the information audit:

- the activity content of IT audit;
- the audit components;
- techniques and tools used to audit information systems.

The activity content of IT audit

Computer audit work includes audits of all major components of a computer system and other processes of the computer system components. In determining the content and conduct of the audit work it is necessary to define the main objective of computer audit and then the main steps of the practical work of the audit team. In general, the computer's audit main objective is to establish and verify that the systems perform their designated duties, as well as the risks for their operation. The stages of development of the IT audit process are relatively similar to those of any audit process. These steps are:

1. audit activities planning;
2. documentation on site;
3. identifying problems;
4. determining solutions to the identified problems;
5. preparing the audit report;
6. elaborating a monitoring graph for tracking identified problems solving.

Computer audit is an independent component of the audit because it audits functioning components of a technical system, which is the computer system, audited with specific techniques and dedicated professionals.

According with U.S. standards, the most important information processes which are audited are the following:

a) the system's internal controls;
b) control over changing software components;
c) control over system safety and recovery in natural or informational disasters;
d) control over the execution of algorithms according to system design specifications.

Audit components

All the components that determine the safe, fair and efficient functioning of the information system are audited. The audit components should address the following processes (Davis, Schiller, et al., 2011):

a) **global auditing** controls in the organization;
b) **Data Centres audit** and disaster recovery techniques;
c) **Audit for filtering devices of information communications**: Internet servers, switches, routers, bridges and Firewalls sites;
d) **auditing operating systems** (Windows operating systems auditing separately, Unix, Linux and web servers);
e) **audit of Databases**;
f) auditing Applications;
g) **auditing wireless networks** (WLAN) and **mobile devices**.

The auditing of computer components is done following specific objectives for each of them and using appropriate audit techniques. Next I will review the audit techniques used for each of the above components.

Global auditing controls across the organization

The specific objective is to check how the development plans of informatics systems are in accordance with the strategic plans of business processes within the organization.

The activities to be checked at a global level refer to: checking the structure of computer business in accordance with the approved structures at the managerial level; identifying performance indicators that measure computer activity; the correlation between system functioning and existing regulations for each informatics process; the possibility and restrictions for the people which are not employees and access the computer system for various controls; the existence of licenses for the computer components used; the remote access to the computer network check; the computer system configuration type for the replacement of components or change of the rules for system management so as it does not cause unnecessary disruption; the mechanism for transportation or labelling of data supports or carries for dispatching from one place to another; the clarity and application of procedures for computer devices acquisition.

Auditing Data Centres and disaster recovery techniques

The specific objective is to check the security level implemented on all activities taking place within the data centre. Security is the most important objective in a data centre because this is the most important data of an organization. The activities audited are: the access of persons in the data centre; alarm systems and their operation; the provision of electricity in case of power failure; the confidentiality measures for the existence and access inside the data centre; the directives, measures, actions and insurances for data centre operation in case of natural disasters, fires or attacks.

Within the Data Centre one should also check: personnel monitoring facilities; rules and responsibilities of individual staff; the responsible in case of emergencies and disaster; protection and data replication techniques; the existence of data replication functional equipment; the rescue storage and duplication of data techniques; the emergency plan and procedures for data recovery in case of emergency, disaster, fire, attacks, etc.

Auditing of computer communications filtering devices

Benchmark audit aims to identify computer networks traffic control rules and information so that only authorized persons have access to available data. To achieve this objective the audit is carried out by using the following activities: identifying the specific network configuration of the informatics network for all equipment used; conformity checks for critical access points of the computer network, in this order: bridges, routers, switches and access filters. The audit of this process includes specific checks of all computer network equipment. For example, checking that all network services which are not needed are disabled; whether the software component of the informatics network management (e.g. SNMP - Simple Network Management Protocol) is a list of

user access control or access to a strong network resource control procedures are defined by roles users type authentication, authorization and user's control. At the level of network equipment some equipment (bridges, routers, switches, etc.) control or filter user access by using encrypted passwords. It is very important, for example, that their network routers do not send out the physical id of the network computer. In order to do this, in the configuration file of the equipment it must be checked that the following commands are included: "no IP source-route" and "no IP directed-broadcast". There are lots of possibilities to manage users and secure passwords, by using encryption or the restriction of traffic on the network.

The auditing of the computer network is done on 4 levels:

a) general network level - where all hardware and software of the computer network is audited;
b) the routers and bridges - auditing if all transfers of network flows are controlled and if dispatching is disabled for IP addresses on the network, but especially outside the network;
c) level switches - to audit how to configure and manage virtual networks, including user control and data flows within virtual networks;
d) Firewalls - checking that all controls are on hold and external attacks on all internal and external IP addresses are filtered accordingly.

Operating systems auditing

The specific objective of the operating system audit is to check how operating systems meet the required processing of applications, such as managed accounts and how user access to the system is controlled. Because operating systems are the most important within computer software packages, their differences between them are so great that each operating system has its own auditing techniques and components. We can identify separate methods and techniques for: auditing Windows-based operating systems that function as servers, operating systems auditing that works as Windows-based workstations in a network (Clients)-like operating systems auditing Unix / Linux and auditing operating systems Web-based servers that provide access to the Internet. In the following I will present only some of the specific audit activities of these operating systems.

Auditing of Windows server operating systems - includes:

- information about the services installed, applications and drivers used;
- the list of programs that start automatically at start-up;
- the security of the system when using direct execution command ("RUN" type), bypassing the operating system interface;
- determining the level of protection of the company by using Firewalls;
- the analysis of system protection resulting from password protection configuration;
- the control of users and programs accessing the operating system;
- the operation and recovery in case of disaster for the operating system.

Auditing of Windows operating systems – client , includes:

- determining the degree of protection by Firewalls;
- determining the types of antivirus programs and the degree of protection which they provide;
- verification of the conditions that the operating system service packs have recommended and regular updates.

Software package "Microsoft Baseline Security Analyzer (MBSA)" deals largely auditing problems of working as a computer workstation (Client).

Auditing of Unix/Linux operating systems – server, includes:

- user and access passwords management;
- auditing control files and file security controls;
- audit of security and control processes for the computer network;

- control of privileged user access ban by logging directly into the operating system;
- security checks so that all users will connect to the automatic control system connection information;
- ensuring that all users connected to the system are monitored;
- operation system security auditing to eliminate the risk of entering the system users, programs, data inconsistent without the standards of the operating system control.

Auditing Web-servers - includes:

- auditing web platform, which refers to operating system security and physical protection of the server and computer network;
- Web server auditing, including basic configuration analysis, used the default settings;
- auditing of Web server applications, which include specific checks accessing pages on the Internet. For example operating system must support at least the standard HTTP, HTTPS, TCP / IP, FTP, SMTP, POP3 and SSL in order to implement basic services on the Internet.

Database Auditing

The specific objective of the audit of databases is that the data are correct and securely stored (http://www.red-database-security.com). The database auditing activities are:

- operating system security database servers, applications and communication;
- access audit roles complexity: passwords, users and access rights;
- independence audit for the database system from the types of operating systems running on computers of "client";
- how the audit system Database Management monitors all activities that occur on the database;
- auditing the encryption techniques used on the database;
- auditing processes to ensure integrity, vulnerability and source processes.

Auditing applications

The specific objective of the audit of applications is to secure their proper functioning. Application auditing activities are (Davis, Schiller, et al., 2011):

- the auditing and control inputs as input or user interface work;
- the auditing of transactions, which seeks to ensure that all operations on the database are executed correctly. Audit Management System seeks to ensure that the database is able to solve any situation that would lead to conducting operations on the database;
- the audit of user access to the applications. This function checks if all levels of protection and user access control are implemented, as follows: at the level of access to the computer network, the operating system level, applications level, the data used and programmed level;
- the auditing of techniques, methods and procedures for application software modification control, including risks arising from them;
- the audit of data protection methods and techniques for their recovery in case of incident or disaster.

Auditing wireless networks (WLAN) and mobile equipment

The audit of wireless networks (WLAN) and mobile equipment's main objective is to check how to protect computer system from outside attacks. A wireless computer network (WIFI) has two distinct components: one with equipment connected by direct physical carriers and another with equipment connected via wireless communication devices. The auditing of component equipment

connected by direct physical support is just as common to all computer networks. For the network that connects wireless devices the auditor should know and follow their specificity. Any wireless user connects to a computer network using two components: the communications equipment: computer, phone, tablets, smartphones, etc., and computer network access point that is a physical network device capable of wireless communication over: computer equipped with "wireless" Internet service provider or telecommunications operator.

The auditing of wireless networks includes the following activities:

- technical auditing of wireless connections, which means checking their individual users requiring network connectivity;
- auditing tools and techniques used for accepting a user network connection;
- the audit of mobile equipment requiring network access.

In this situation we must have more sophisticated SOFTWARE means to identify the work and safety protocols for applicant identification. In this case the applicant's personality should be monitored, also that of the connecting mobile equipment, of the machine owner, the equipment manufacturer and user accounts associated with the respective user.

Techniques and tools used to audit information systems

The entire information systems audit work is performed with specific equipment and especially with dedicated software for auditing various activities, functions and system equipment components. Their detailed presentation requires more specific knowledge of each product use program. For example I will present only the product MBSA (Microsoft Baseline Security Analyzer) for auditing on a Windows station "client" (http://www.microsoft.com/download/en/detailsaspx?id=7558). Program highlights for a computer or a computer network administrator errors that can cause instability in the operation system. MBSA in terms of audit work carried out following checks:

- the danger level of existing passwords;
- the hazard level and the file management system (NTFS);
- the file management system used and the danger presented for each drive;
- the analysis and control of user access to the operating system: if no password is allowed auto-start, if allowed to connect to your computer with password visitor, if allowed to use a generic password as anonymous.

Figure 1 illustrates the MBSA (Microsoft Baseline Security Analyzer) start program execution.

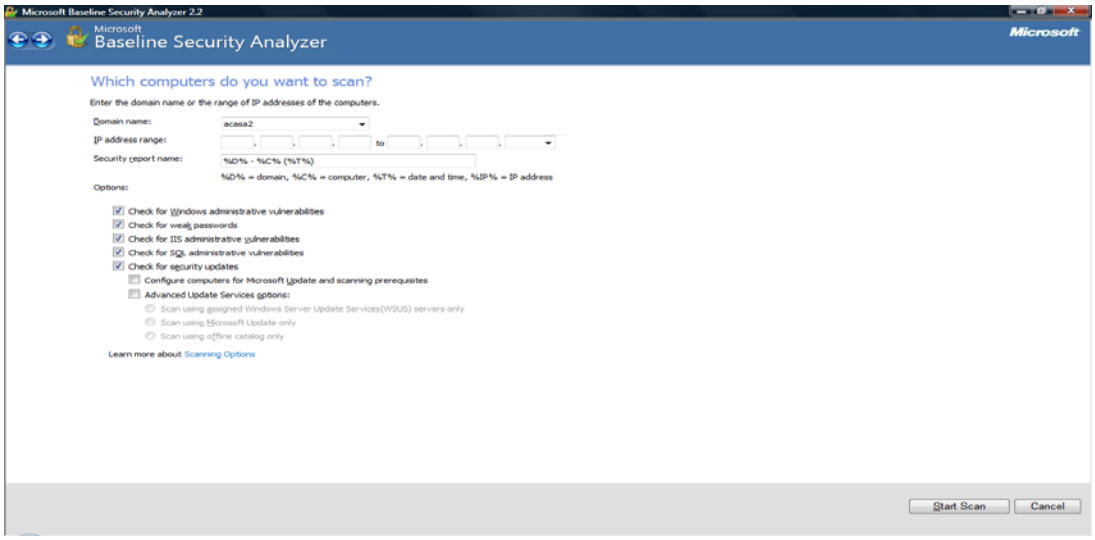

Figure no. 1 – The MBSA the start program execution.

After analyzing a computer from the network, the complete results are obtained for the full audit of the Windows client station USER-PC workgroup network group. Fig. no. 2 presents an extract from the analysis result where we can observe the greatest vulnerabilities found, for example, Windows has 5 updates missing and did not installed a service pack, Office software package has 8 updates missing and three Service Packs not installed, so.

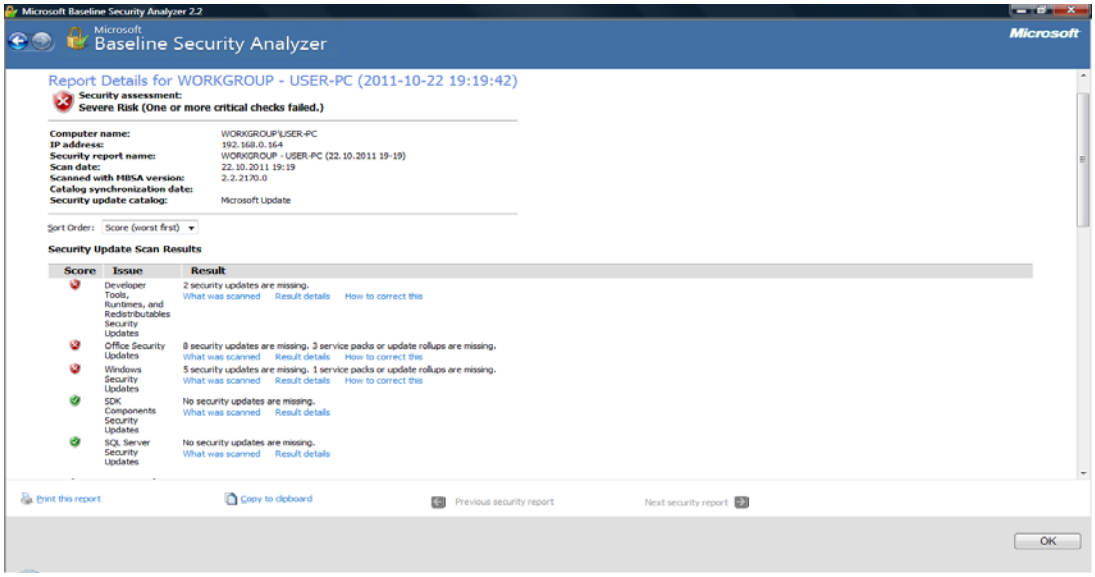

Figure no. 2 – MBSA - The Problems identified in the computer system security

If you want to see the detailed content of their errors or missing components give a simple click on the report and see the mores details of the problems identified as nonconformities that irregularities and their degree of hazard, critical or important (see fig.no. 3). Based on these reports automatically obtained the auditor prepare audit report stating the situation and propose appropriate measures to remedy dangerous situations or shortcomings.

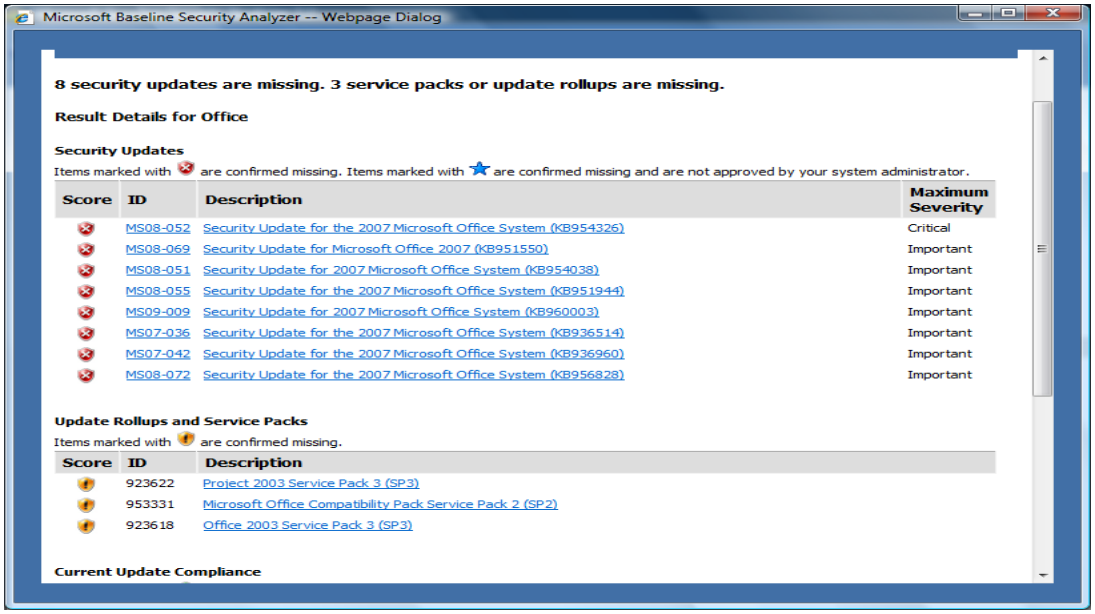

Figure no. 3 – MBSA- Detailed description of the shortcomings found in Office software package

We need to know that the audit program suggests solutions to problems identified, as shown in fig. 4.

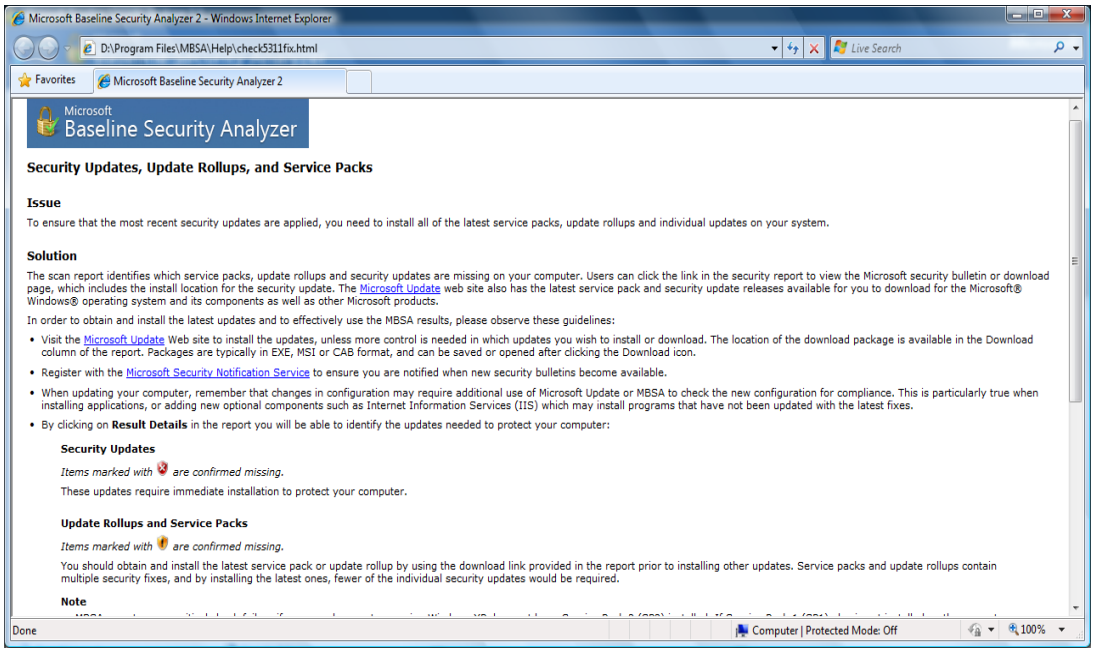

Figure no. 4 – MBSA – ways to solve problems according to the type and degree of risk

This example shows that globally, for auditing computer systems many steps forward have been taken and that there is software that makes it easier for auditing information. As seen from the above example in the delivery of audit software there is still room for improvement.

Conclusions

This paper brings to the attention of economists and computer specialists computer the issue of informatics auditing by providing detailed audit objectives, IT activities to be audited and techniques used in auditing information systems. After their description, the possibilities for implementation are presented for the audit of informatics systems. As resulted from the practical study presented, informatics products for auditing purposes are still emerging and there is need to integrate them within software systems for auditing informatics systems. The brief example of auditing a Windows computer running as a network client computer practically demonstrates the need for this work to be done by economic informatics specialists. I emphasize that because the correct interpretation of results and retention of necessary measures according to their gravity can only be done by people who understand the operation of an information system's complexity. I want to emphasize that the use of over-specialized people such as programmers, or of some too little specialized, such as economists, could lead to the misinterpretation of findings, especially for the audit of operations systems, databases and wireless networks.

From the description, above, the activities to audit and audit software means that information systems used is a specific audit activities and techniques that do not occur in other types of audit. The conclusion of this work is that informatics audit represents a specific audit and not be confused or substituted by internal audit or financial audit.

References

1. Davis C., Schiller M., Wheeler K., 2007. IT AUDITING, using controls to protect information assets, The McGraw-Hill companies, Osborne, New York, USA
2. Dănescu T., 2007. Audit financiar: convergente intre teorie si practica, IRECSON Publishing House, Bucureşti
3. Eden A., Stanciu V., 2004. Auditul sistemelor informatice, Dual tech Publishing House, Bucureşti
4. Renard J., 2003. Teoria si practica auditului intern, Ministerului de Finanțe Publishing House, Bucureşti
5. Rus I., Dănescu T., 2010. The Information Audit – between necessity and regulation, in APPLIED ECONOMICS, BUSINESS & DEVELOPMENT, 2010, Kantaoui, Sousse, TUNISIA, available online at http://www.wseas.org, p.98-103
6. http://www.red-database-security.com , 22/10/2011
7. http://www.microsoft.com/download/en/ details. aspx?id=7558 , 22/10/2011
8. https://www.isaca.org/CERTIFICATION/Pages/default.aspx , 22/05/2012