THE AUDIT PROCESS OF THE IT SYSTEMS OF A COMPANY THAT PROVIDES ACCOUNTING SERVICES

Laura – Eugenia – Lavinia Barna*
The Bucharest University of Economic Studies, Bucharest, Romania.

Abstract
Over the time, IT systems have constantly evolved and for this reason IT systems must undergo periodic audit procedures to see if they enable the achievement of a company's strategic objectives and the efficient use of IT resources. The main purpose of the paper is to investigate how the audit mission is carried out on IT systems (ERP systems) within a company that provides accounting, consulting, payroll and audit services. The role of these IT systems (ERP systems) is to ensure the correct and complete integration of information within a company. ERP systems provide the perfect maintenance of the internal control system, but also the ability of managers to analyse the information provided by these IT systems as correctly as possible.
In this article, the author made a case study, analysing the risks of an IT system of a company that offers accounting services using the MEHARI technique. The results obtained showed that the systems are effective and would withstand cyber-attacks, but could be less resistant in terms of specialized attacks (well-equipped hackers, professional spies).

Keywords
audit, ERP systems, mission, accounting, objectives, information.

JEL Classification
M15, M19, M41, M42

Introduction

As a result of the significant evolution of IT systems, more and more companies in the economic field have started to implement IT systems (ERP systems). ERP systems are implemented with the goal of integrating information from the entire company. The benefits of companies that have decided to implement ERP systems are that these systems provide *"easy maintenance of internal controls"* (Matsuo, 2009; Nikkei Solution Business, 2009 cited by Okuda and Nakashima, 2015). ERP systems help

* Corresponding author, **Laura – Eugenia – Lavinia Barna** – laura.barna@cig.ase.ro

companies to get data or information as accurate as possible after processing and to achieve the most correct and logical flow of information while ensuring information transparency.
The role of these ERP systems is to translate the company's transactions and activity into the system's database (Okuda and Nakashima, 2015), so that more and more departments of the company have access to the relevant information needed to carry out daily activities.
However, the entire activity of a company must be closely monitored through IT system audit missions (Dash et al., 2019). According to Mittelstadt (2016), the audit process *"is considered a possible mechanism to achieve transparency [...] and to verify the correct functioning of the system"*.
This article aims to highlight the way to analyze the activity of a company that provides accounting services using the MEHARI technique in the process of auditing the company's activity. The main purpose of the paper is to investigate how the audit mission is carried out on IT systems (ERP systems) within a company that provides accounting, consulting, payroll and audit services. In this article is presented a faithful analysis of the security in which the company's IT equipment and activities are at a given moment, offering minimal recommendations regarding the improvement or replacement of certain IT components to increase the company's security level.
The article is structured in 4 parts as follows: a section related to the review of specialized literature where the main concepts and articles dealing with the subject of IT systems audit missions were reviewed, a section that develops the research method used (based on studying the activity of a companies that provide accounting services), an analysis section of the results obtained on the basis of two areas found in the MEHARI technique and a conclusion section that develops the idea of the need for IT audit missions.

1. Review of the scientific literature

The implementation of ERP systems within companies in the accounting field has gained momentum as a result of the increase in the degree of digitization of a large number of activities (Rîndașu, 2018). Srivardhana and Pawlowski (2007), state that the implementation of ERP systems *"offers new opportunities by developing different common cognitive structures for employees from different functional areas"*, giving the company the opportunity to develop effective innovative processes.
ERP systems are defined as *"a single, useful platform for the integrated monitoring, control and management of all activities, processes and operations carried out by a company"* (Transart, 2021). The use of ERP systems continuously improves the flow of information between departments, so that the activities within the company are carried out much more efficiently.
The activities carried out by employees in the ERP systems must be constantly monitored through audit missions of the IT systems, with the aim of ensuring effective control over data access, as well as a superior quality of the data that will be the basis of decision-making.

According to Popescu (2019), the audit mission represents *"an achievement that has a definable objective, consumes resources and is constrained by elements such as time, costs and quality"*. The main purpose of the audit missions is to reduce the estimated level of analysis and control errors of the audited IT systems. This audit process is carried out annually iteratively, so that errors have the lowest possible threshold, and conclusions from previous missions are the basis of the current audit mission.
Figure no. 1 shows the main stages of an accounting information systems audit mission:

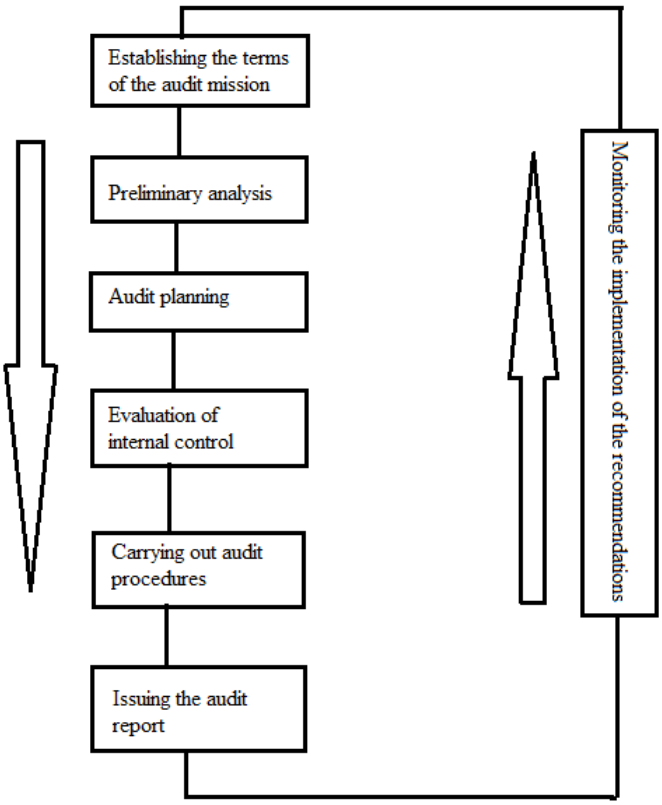

Figure no. 1. Stages of the audit mission
Source: Popescu, 2019

Establishing the terms of the audit mission gives the auditor the opportunity to establish the purpose and objectives underlying the relationship between the auditor and the audited company. The engagement letter should contain the duties, authority and responsibility of the auditor.
In the audit mission, the auditors must have access to all relevant information both about the company and about the activity carried out by it. Also, all stages of an IT systems audit mission must be completed.

According to Horomnea and Chiru (2011), an IT systems audit consists of an examination of the controls applied to the infrastructure of an IT system. These reviews can be performed either with an audit of the financial statements or with an internal audit. The main purpose of IT audit is to observe whether IT systems *"protect company assets, maintain data integrity and operate efficiently"* (Horomnea and Chiru, 2011, p. 362) so as to achieve a company's objectives.
The information an auditor needs to obtain about a company's IT environment is:
a). IT resources used by the company (IT department staff, IT equipment, data storage, software used, company access systems);
b). operations performed with the help of computer equipment;
c). relationship and exchange of information between departments;
d). processing carried out outside the company.

2. Research methodology

In the article, the author used the MEHARI technique to identify whether the IT systems used keep data stored correctly and securely.
The MEHARI technique is based on a questionnaire consisting of a series of questions. Questions are related to the effectiveness and robustness of security measures. These sets of questions are specific to each domain to make the assessment as effective as possible. The areas chosen for analysis were: ***security organization*** and ***website security*** (the IT application used being stored in the Cloud). The reason why the 2 fields were chosen is to evaluate how the data is kept both in physical and online format.
For the analysis, author chose B&B Consulting (the real name of the company was anonymized), which operates in the field of accounting services, having been established 20 years ago and having a large portfolio of clients. The upward evolution of the company is due to the activity supported by basic principles such as: identifying and fulfilling customer requirements, quality in business, business ethics and the quality of services offered. The chosen company has 120 employees, the team is constantly developing.
If the company's IT system is analysed, the main points would be:
a) access to the company: based on the access card
b) information confidentiality and restricted access areas: all customer data is kept in cabinets. Sensitive data is stored in locked cabinets (cabinets with special regime).
c) distribution of keys: each cabinet is provided with 2 keys. If it is not necessary to lock the cabinet, a key remains with the cabinet. The duplicate key can be found at the manager of the logistics department. The keys to the special regime lockers are available from the executive director.
d) communication within the company: it is carried out on the basis of the internal IT application with numerous functions, found on the company's internal web page (intranet).
e) scanners: allow documents to be scanned and sent via email or laptop. For scanning, one user account is used on each scanner (only IT department employees can create an account on each scanner).

f) physical archiving of documents: correct archiving of accounting documents in accordance with the client's requirements
g) daily report using the IT application:

- eliminating errors from the daily activity reports;
- correct calculation of salary rights based on attendance and daily reporting;
- obtaining information on the number of hours worked on each client;
- increasing the efficiency with which individual working time is used;
- increasing labour productivity.

3. Results and discussions

The areas analysed in the case study of B&B Consulting (the real name was anonymized) using ERP systems were:
1. Security organization
2. Website Security

For the first domain ***"Security organization"***, general aspects within the company were analysed such as: security ensured within the company, system security, information protection, resource management, asset management, human resource management, adequate staff training, as well as plans for continuity business (Table no. 1).

Table no. 1. Security organization

Subdomain	Possible values (W) *	Active sum (r*W)	Average
01A - The role and structure of security	106	84	3,17
01B - Security Reference Guide	115	99	3,44
01C - Human resources management	125	113	3,62
01D - Insurance	117	87	2,97
01E - Business continuity	64	55	3,44
Results	527	438	3,32

Source: Author's own creation, 2023

*Possible values given by the auditors to each question in the MEHARI questionnaire

In the questionnaire used for this area, we identified that policies and work procedures are implemented correctly and security management actions are checked monthly. The security policy is reviewed periodically so that the risk of incidents is minimized. The security rules are also presented through periodically organized internal courses, and the company's employees have access to the work procedures to ensure an increased degree of data security.

In addition to the confidentiality clauses in the employment contract, there is also the employee handbook, which also outlines security principles. Also, all employees have access to work procedures stored on the intranet. Access to applications or information is only possible based on your username and password.

For the second area ***"Website Security"***, general aspects of the company were analysed such as: access control in the building, risk analysis, access control in different areas of the office, detection of intruders in office spaces, protected information, ways of securing correspondence (Table no. 2).

Table no. 2. Website security

Subdomain	Possible values (W)*	Active sum (r*W)	Average
02A - Access control in the premises and building	104	80	3,08
02B - Protection against various environmental risks	4	4	4
02C - Access control in office areas	142	99	2,79
02D - Protection of written information	173	130	3,01
Results	423	313	2,96

Source: Author's own creation, 2023

*Possible values given by the auditors to each question in the MEHARI questionnaire

The company's IT department has a list of all users so that all employees who have access to data are known, thus ensuring better control over sensitive information. There is also an operational intruder detection system.

The average of the 2 domains analysed is 3.16 (level 3), illustrating that the server is more efficient and resistant to attacks and events, but it could be insufficient against specialized attacks (well-equipped and experienced hackers, professional spies) or disasters natural.

The author also carried out a SWOT analysis based on information from within the company, arguing with relevant examples presented in table no. 3.

Table no. 3. SWOT analysis

SWOT analysis	Example
Strengths	- secure access within the company - secure access within applications - the clear delimitation of work processes by components, their grouping by positions and departments; - establishing certain managerial, economic and technical criteria;
Weaknesses	- the absence of any restrictions on the introduction of new storage media (anyone can insert any storage medium into computers without notifying the persons

	responsible for the management of the storage media)
Opportunities	- possibilities to avoid data loss as a result of natural disasters: fires, floods, earthquakes - possibilities to avoid data loss as a result of unexpected software/hardware errors - possibilities to avoid data loss as a result of unintended actions of staff
Threats	- the flexibility of the legislative framework - free movement of services and people

Source: Author's own creation, 2023

Caraiman (2015) found that ERP systems can provide a number of benefits:

• Reduction of stocks
• Reduction of material expenses
• Reduction of labor costs
• Improving sales and customer relations
• Better control over accounting and receivables
• Reduction of operational costs
• Facilitates the management of current operations
• Stock optimization
• Increasing the level of order fulfillment
• Improving cash flow
• Integration of financial information

Thus, for the proper functioning of these ERP systems, the periodic organization of the IT audit is necessary.

The obtained results aim to reveal which aspects should mainly be followed in order to ensure an advanced security of both data and employees in certain situations, which was followed using the MEHARI technique.

Conclusion

The purpose of reporting is to highlight control weaknesses identified by the auditor and bring them to the attention of the audited entity through the audit report and a letter containing a summary of key findings and recommendations. The audit report identifies the scope, objectives, period, time planning and coverage area of the audit activity performed. According to Cristescu and Stancu (2019), the audit report *"must contain a clear opinion based on the conclusions of the company's audit process"*. Other characteristics identified by Cristescu and Stancu (2019) were the *"ease of understanding the report"* or the presentation of a *"clear, complete and concise idea"* regarding the situation of the IT equipment and systems used.

However, Hammer (2007) and Nwankpa and Datta (2012) concluded that the implementation phase of ERP systems is more successful if that company goes through the audit process first. The reason why these authors reached this conclusion was the way in which the approach to the audit mission is carried out: the technical endowment,

the communication infrastructure, the way of organizing and the structure of the IT staff and the ongoing development projects are analysed. In addition to these, periodic inspection of ERP systems would contribute to ensuring the quality and security of data processed with ERP systems (Murumba and Machii, 2020).

For the company chosen in the case study, all information was collected by direct observation of the working spaces where the equipment and servers are installed, examination of the technical-economic documentation, internal discussions with people from the IT department and examination of the company website situation.

Following the analysis, the author came to the conclusion that this company has adequate controls, personal information and those classified strictly secret are confidential, but also efficient management of human, financial, material and time resources. However, there is still the possibility of being vulnerable to powerful cyber attacks.

As a recommendation, it would be the implementation of some restrictions on the use of storage media, and the technical documentation to be more explicit so that it can be easily understood by a person who has no experience in this field.

The limitation of the study consisted in the fact that only one company was chosen for the MEHARI analysis, due to the limited access to confidential security data of the companies.

References

[1] Caraiman, A.C., 2015, *Advantages and Disadvantages of Using Integrated ERP Systems at Trade Entities*. Annals of the "Constantin Brâncuși" University of Târgu Jiu, Economy Series, 4, pp. 170-174

[2] Cristescu, M.P., Stancu, A.M.R., 2019, *Trends in Auditing ERP Systems*. Knowledge Horizons – Economics, 11(4), pp. 46-53

[3] Dash, A., Mukherjee, A., Ghosh, S., 2019, *A Network-centric Framework for Auditing Recommendation Systems*. DOI: https://doi.org/10.48550/arXiv.1902.02710

[4] Hammer, M., 2007, *The Process Audit*, Harvard Business Review, 1, pp. 1-14

[5] Horomnea, E., Chiru, S.C., 2011, *Auditul sistemelor informatice [IT systems audit]*, Available at: proceedings.univ-danubius.ro/index.php/eirp/article/download/932/851

[6] Mittelstadt, B., 2016, *Auditing for Tranparency in Content Personalization Systems*. International Journal of Communication, 10, pp. 4991-5002

[7] Murumba, J., Machii, J.K., 2020, *ERP Software Inspections and Audits*. IGI Global, DOI: 10.4018/978-1-5225-7678-5.ch013

[8] Nwankpa, J., Datta, P., 2012, *Perceived Audit Quality from ERP Implementations*. Information Resources Management Journal, 25(1), pp. 61-80

[9] Okuda, S., Nakashima, M., 2015, *Systems Integration, Management Involvement and Quality of Internal Controls and Auditing*, Asia-Pacific Management Accounting Journal, 10(1), pp. 1-21

[10] Popescu, G., 2019, Course support: *Auditul și Controlul Sistemelor Informaționale [Information systems audit and control]*

[11] Rîndașu, S.M., 2018, *Information security challenges – vulnerabilities brought by ERP applications and cloud platforms*, Audit Financiar, 16(1(149)), pp. 131-139, DOI: 10.20869/AUDITF/2018/149/005

[12] Srivardhana, T., Pawlowski, S.D., 2007. *ERP systems as an enabler of sustained business process innovation: A knowledge-based view*, Journal of Strategic Information Systems, 16, pp. 51–69
[13] Transart, 2021, *Ce este un sistem ERP? | Beneficiile și componentele unei aplicații ERP [What is an ERP system? | Benefits and components of an ERP application]*. Available at: https://www.transart.ro/ce-inseamna-erp/, accessed on April 10, 2023