

Ensuring the Security of Financial-Accounting Data Stored in the Database of ERP Systems

*Laura-Eugenia-Lavinia BARNA,
Ph.D. Student, Bucharest University of Economic Studies,
Accounting Doctoral School,
e-mail: barnalaura15@stud.ase.ro*

*Prof. Univ. Bogdan-Ştefan IONESCU,
Ph.D., Bucharest University of Economic Studies,
Management Informatics Systems Department,
e-mail: bogdan.ionescu@cig.ase.ro*

Abstract

The accounting profession is in a continuous digitization process, as a result of the frequent use of computer systems with the aim of streamlining and improving the daily activity of employees in this field. However, in addition to the benefits offered by these IT systems for accounting professionals, the risks to which the information processed and stored with these IT systems could be subjected must also be taken into account so that the quality of financial-accounting activities is not disturbed.

The present work aims to analyze the main risks to which the financial-accounting data processed and stored in the database of the ERP systems could be subjected, as well as the way to ensure the security of the financial-accounting data within these integrated IT solutions. This article focused on a quantitative research using bibliometric analysis which is basically based on the analysis of a sample of 263 articles dealing with the two key topics of the paper: "data security" and "ERP systems".

Key words: risk; data security; ERP systems; integrated IT solutions; digitization; bibliometric analysis;

JEL Classification: G32, L86, M15, M40, M41

To cite this article:

Barna, L.-E.-L., Ionescu, B.-Ş., (2023), Ensuring the Security of Financial-Accounting Data Stored in the Database of ERP Systems, *Audit Financiar*, vol. XXI, no. 2(170)/2023, pp. 291-299, DOI: 10.20869/AUDITF/2023/170/008

To link this article:

<http://dx.doi.org/10.20869/AUDITF/2023/170/008>

Received: 23.03.2023

Revised: 31.03.2023

Accepted: 2.05.2023

Introduction

The technological evolution of recent years has determined the digitization of a large number of activities both in the financial-accounting field and in other fields, thus facilitating the processing, analysis and storage of a large volume of information in a shorter period of time as a result of the use of IT systems. However, the data must be kept safe from the moment of their introduction into the IT systems until the moment of their storage, processing and analysis, because recently "users have become the most vulnerable link of security systems" (Popescu and Popescu, 2018).

The specialized literature associates this technological evolution with an important factor in the increase in the number of IT security threats. However, ensuring adequate controls and a protection system would be of great help in ensuring the security of financial-accounting data stored in IT systems.

The purpose of the paper is to identify the main measures that can be adopted, so that the financial-accounting information processed and stored in the database is not subject to risks arising from the online environment.

1. Literature review

1.1. The importance of ERP systems in the financial-accounting activity

The ERP (Enterprise Resource Planning) system is an integrated IT system used by companies to manage a large volume of data and resources (Pareek, 2014; Hrischev, 2020; Kitsantas, 2022). According to Senior Software (2020), the ERP system allows "the integrated management of processes and operations from different business areas: purchases, sales, accounting, production, customer relationship management, project management, but also other logistics activities".

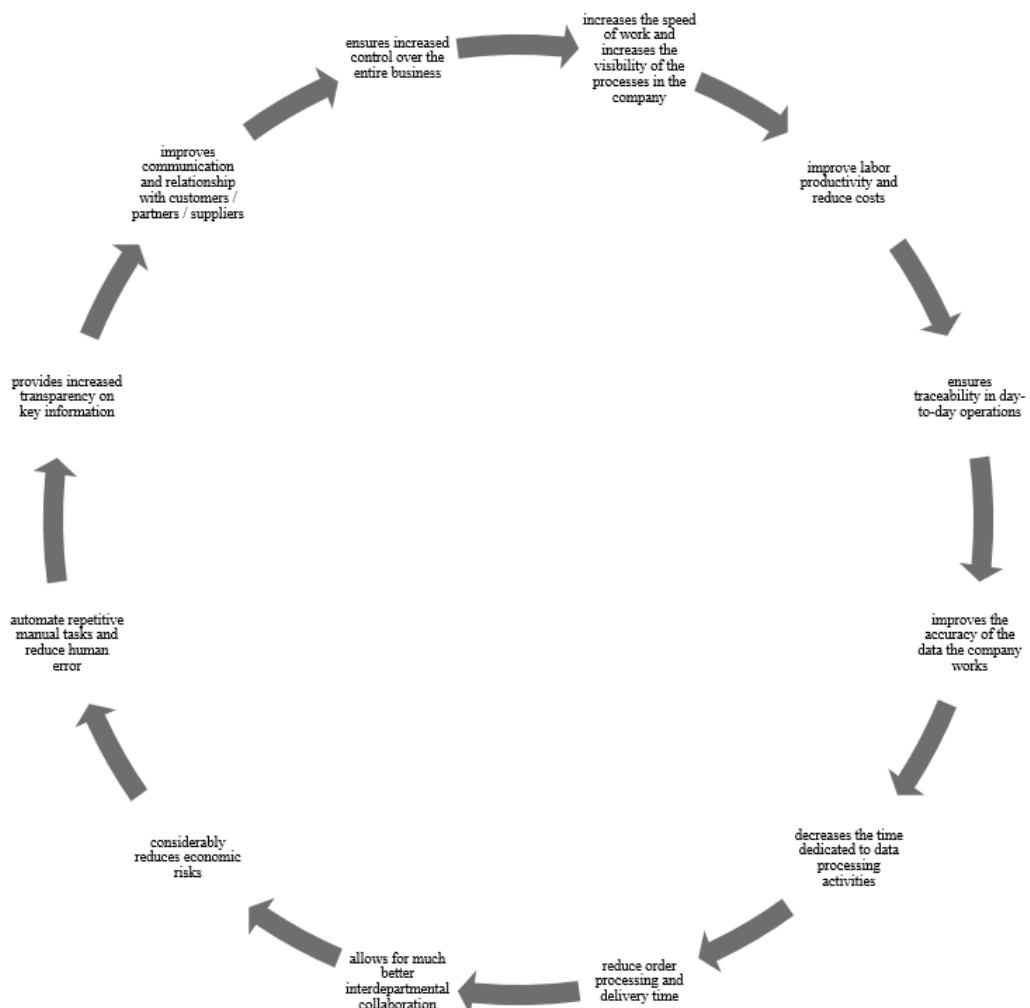
Many companies operating in the financial-accounting field decide to implement these ERP systems, because it gives them centralized access to essential data for the company, allowing the automation of a wide range of operations that streamlines the flow of information. Moreover, ERP systems offer users the possibility to enter data directly from the keyboard, either to import the data, or to use the transfer technology through EDI (Electronic Data Interchange) technology. The main functionalities of ERP systems that lead companies to implement these IT solutions are:

- the entire flow of information within the company is recorded in the common database of the ERP system;
- ensures the automation and standardization of various operational processes;
- ensures monitoring of activities and resources used by the company;
- electronic generation of various financial and accounting documents (invoices, statements, accounting notes);
- manages the financial operations within the company;
- generates various reports necessary for the financial-accounting department, but also for other departments of the company.

The main benefits offered by ERP systems for companies are presented in *Figure no. 1*.

Kanelou (2013) identified three relevant reasons why companies decide to implement ERP systems: "the increased demand for real-time information, the generation of information for decision-making and the need for application integration". Nawaz and Channakeshavalu (2013) also identified other benefits: business process reengineering, standardization of systems and processes, improved practices.

Figure no. 1. The benefits of ERP systems



Source: Author's creation, 2022

1.2. The main categories of risks to which financial and accounting data processed and stored in ERP systems can be subjected

According to Popescu and Popescu (2018), the main types of cyber risks / attacks that a company can face are:

- attacks on applications;
- cyber espionage (unauthorized access to data processed using ERP systems);
- theft or physical loss of equipment;
- soft malware;

- errors;
- incorrect business process mapping.

1.3. The main measures to ensure the security of financial-accounting data stored in the database of ERP systems

The main levels of data security which any computer system should have are: physical security, logical security, access security, service security. Access security is defined in the specialized literature as the way users access the

system. In this way, controlled access to sensitive data within the company can be ensured. The security of the services requires that the detection and warning functions in case of a potential cyber-attack or data theft are activated throughout the use of the computer system.

Hrishev (2020) and Parthiban and Nataraj (2019) observed that the first step in ensuring data security in the database of ERP systems is the system architecture, in other words the way in which that information system is designed. ERP systems present an architecture based on three levels:

- *the presentation level* – the terminals, where data is entered and transferred between levels
- *application level* – the IT system server (data processing based on algorithms and business functions)
- *database level* – database server of the IT system (data storage area)

Among the measures that can be adopted to ensure the security of financial data stored in the database of ERP systems could be (Chang et al., 2014):

- controlled access to data, so each user has access only to the data they use on a daily basis;
- the level of data sharing is strictly defined so that the data confidentiality procedure is not violated;
- data communication to customers is carried out through well-defined and secure communication channels (eg: SharePoint, Google Drive, etc.) and are well encrypted

Another step would be to ensure a stable and encrypted internet connection (She and Thuraisingham, 2007; Sorheller, 2018) so that the risk of data theft is minimized.

2. Research methodology

The research method used by the authors in this article aimed to define the concept of security of financial-accounting information processed and stored in the database of the ERP system with the help of scientific articles dealing with this subject. The articles were collected between October 29, 2022 and November 5, 2022 from different databases such as: Web of Science, Scopus,

Emerald, Elsevier and other databases, using the following search keywords: "data security", "ERP systems", "financial-accounting data stored in ERP systems", "security of databases", "security of ERP systems".

The authors also constructed some research questions presented below regarding the topic of the article, trying to answer them with the help of the information collected from the selected articles:

- Q1. *What is the framework for ensuring internal control?*
- Q2. *What are the benefits offered to users of ERP systems?*

- Q3. *What are the main solutions to ensure the security of financial-accounting data?*

Thus, to quantify the results related to the security of ERP systems, the authors used a bibliometric analysis focused on the grouping of the keywords "security" and "ERP systems" in relation to other keywords identified in the selected articles from the Web of Science platform. The sample consisted of 263 articles relevant to the subject of the paper, published between 1996 and 2022, most of them being published after 2012, when the massive evolution of the concept of digitization of activities took place. To process the data on the selected articles, the authors used the VOS viewer application. The obtained results are presented in the next section.

3. Results analysis

Analyzing the 20 articles selected from different databases, the authors identified a series of information relevant to the topic of the article. To the question "*What is the framework for ensuring internal control?*", the authors Chang (2014) and Chang et al. (2014) identified the fact that system security and internal controls in ERP systems are ensured by "security policy, user authentication method, database security". The controls applied maintain the reliability of the IT system, but also the availability of financial data. However, the authors Chang et al. (2014) defined the framework for ensuring internal control through 5 components presented in *Figure no. 2*.

Figure no. 2. The framework for ensuring internal control



Source: Author's creation based on Chang et al. (2014)

Hrischev (2020) states that each user must have controlled access to data within the database. Most ERP systems use the Citrix application that contains an infrastructure that secures information on the Internet using an access portal (Gateway) with a username and password, thus increasing data security.

The database of the ERP system is structured either by SQL (Structured Query Language) or Oracle DB. New versions of ERP systems use NoSQL databases, ensuring a higher degree of security.

To the question "What are the benefits offered to users of ERP systems?", the author Kanellou (2013) states that ERP systems offer users an increase in the flexibility of information, the improvement of the quality of reports, but also the improvement of the decision-making process. Kitsantas (2022) identified that ERP systems provide better information in a shorter time, at a lower cost. Other authors are of the opinion that the implementation of ERP systems is quite expensive, but along the way this investment made by the company is amortized. Nawaz (2013) believes that ERP systems offer users the opportunity to process information much faster, but also to centralize data much more efficiently as a result of the integration of a large number of functions that ERP

systems have, useful functions for different departments in within the companies.

The authors Pareek (2014), Onyshchenko (2018), Rîndașu (2018) and Parthiban and Nataraj (2019), believe that the main measures for data security in ERP systems are: Internet network security (applying an HTTPS protocol, ensuring user authentication based of digital certificates), database security (isolation of the server from the rest of the company's IT infrastructure), application server security, information security on the used terminals and ERP systems security.

She and Thuraisingham (2007) and Sharma and Maheshwari (2014) are of the opinion that financial-accounting data security should first be ensured from inside and outside the company and proper internal control of the ERP system should be ensured. Also, a recovery plan should be designed in the event of a cyber-attack or data theft (Xu et al., 2002; Weng and Hung, 2014).

The FBI (2012, cited by Mangiuc, 2016) identified the following sources of IT security risk as mainly disgruntled employees, then independent hackers or economic espionage and business intelligence.

To the question "*What are the main solutions to ensure the security of financial-accounting data?*"¹, the author Rădulescu (2016) identified the following security solutions for a company's data on the following levels:

- *logic*: encryption, backup, monitoring, antivirus, audit, firewall
 - *physical*: securing managed equipment
 - *operational-administrative*: creation of working procedures, trainings with employees, etc.

According to the study carried out by Rîndaşu (2019), the majority of accounting professionals who have been the target of a cyber-attack most often contact the IT department of the company. Other accounting

professionals turn to their line manager, data protection officer, authorities or colleagues to resolve issues arising from the cyber-attack.

Analyzing in detail the identified information, the authors of this article believe that the security of financial-accounting data should be ensured both inside the company and outside it.

In *Figure no. 3*, the data on the 263 articles selected from the Web of Science based on the keywords "security" and "ERP systems" in relation to other keywords, show that many articles present the security of ERP systems from the perspective of new technologies such as: cloud computing, Big Data, e-business, SaaS.

Figure no. 3. The relationship between the keywords "security" and "ERP systems"



Source: Authors' creation based on information collected about articles from the Web of Science platform (2023)

The authors identified 7 groups of keywords (clusters), which are presented in detail in Table no. 1. The clusters that registered the most items show shades of intense black, following gradually, with the

decrease in the number of items, this shade to predominate in shades of dark gray and light gray. Thus, clusters containing the fewest elements show a very light gray shade.

Table no. 1. Keyword clusters identified in the selected articles

Groups (Cluster)	Specific keywords
Cluster 1 (9 items)	Big Data, Blockchain, Cybersecurity, Information security, Internet, Management, Privacy, Security, Systems
Cluster 2 (10 items)	Adoption, Cloud, Cloud computing, Determinants, E-business, Information-technology, Performance, SaaS, Smes, User acceptance
Cluster 3 (7 items)	ERP implementation, Information systems, Integration, Model, Optimization, Success, Technology
Cluster 4 (7 items)	Business, Challenges, Cloud ERP, Critical success factors, Enterprise, Network, Network security
Cluster 5 (7 items)	Authentication, Classification, Data security, EEG, ERP, P300, RFID
Cluster 6 (6 items)	Enterprise systems, Framework, Impact, Implementation, Internal control, Software
Cluster 7 (1 item)	Services

Source: Author's creation

As can be seen in **Table no. 1**, the keywords identified are related to each other, all words refer to new technologies in the IT field. Thus, the correlation identified by the authors would be mostly between

ERP systems, security, authentication and implementation.

Table no. 2 shows the distribution of publications and their citations by geographic region.

Table no. 2. Distribution of publications and their citations by geographic region

Country / geographic region	Number of papers written in each country / region	The number of citations of articles originating from that region
USA	45	996
China	47	314
India	34	198
Anglia	17	693
Saudi Arabia	9	142
Taiwan	19	97
Germany	16	203
Italy	5	46
Australia	6	171
Canada	8	204
South Africa	8	44
South Korea	8	138
Pakistan	5	29
Spain	6	68
Czech Republic	5	11
Indonesia	6	3
Polonia	7	20
Romania	7	16
Ukraine	5	9
TOTAL	263	3402

Source: Author's creation

Most articles come from countries developed in terms of digitization such as: China, USA, India, Taiwan, England and Germany. The other countries such as Italy, Australia, Canada, South Africa, South Korea, Pakistan, Spain, Czech Republic, Indonesia, Poland, Romania, Ukraine register a small number of articles, between 5 and 8 articles per country or region.

4. Conclusions

Even if the digitization process has gained momentum in recent years, the provision of adequate security of the data processed and stored with these ERP systems must also be taken into account.

The digitization of activities in the financial-accounting field emerged as a result of the need for users to have quick access to relevant information in real time.

As a result of the post-pandemic effects of COVID-19, there has been an increase in the number of security incidents both nationally and globally according to the report issued by CERT. How to reduce the occurrence of such an incident is still under investigation. Technological progress has influenced the appearance of new categories of vulnerabilities in ensuring data security.

Considering the articles selected to substantiate the theoretical basis of the present article, the authors concluded that a stable and strong organizational culture can prevent the occurrence of security incidents, because the flow of information is much better managed by the members of such an organization, and the activities are much better defined within the organization.

REFERENCES

1. Chang, S.I. (2014), Internal control framework for a compliant ERP system, *Information & Management*, vol. 51, pp. 187-205, DOI: <http://dx.doi.org/10.1016/j.im.2013.11.002>
2. Chang, S.I., Yen, D.C., Chang, I.C., Jan, D (2014), Internal control framework for a compliant ERP system, *Information & Management*, vol. 51, pp. 187-205, DOI: <http://dx.doi.org/10.1016/j.im.2013.11.002>
3. Hrischev, R. (2020), ERP systems and data security, *IOP Conference Series: Materials Science and Engineering*, vol. 878, pp. 1-8
4. Kanellou, A., Spathis, C. (2013), Accounting benefits and satisfaction in an ERP environment, *International Journal of Accounting Information Systems*, vol. 14, pp. 209-234, DOI: <http://dx.doi.org/10.1016/j.accinf.2012.12.002>
5. Kitsantas, T. (2022), Exploring Blockchain Technology and Enterprise Resource Planning System: Business and Technical Aspects, Current Problems and Future Perspectives, *Sustainability*, vol. 14, DOI: <https://doi.org/10.3390/su14137633>
6. Mangiuc, D.M. (2016), Auditing security for the Cloud, *Audit Financiar*, vol. XIV, nr. 3 (135) / 2016, pp. 302-311, DOI: <10.20869/AUDITF/2016/135/302>
7. Nawaz, M.N., Channakeshavalu, K. (2013), The impact of Enterprise Resource Planning (ERP) systems implementation on business performance, *Asia Pacific Journal of Research*, vol. 2, nr. 4, pp. 30-47
8. Onyshchenko, O. (2018), Introducing ERP system as a condition of information security and accounting system transformation, *International Journal of Engineering & Technology*, vol. 7, nr. 4.3, pp. 530-536
9. Pareek, R. (2014), Analytical Study of Cloud ERP and ERP, *International Journal of Engineering and Computer Science*, vol. 3, nr. 10, pp. 8710-8717
10. Parthiban, K., Nataraj, R.V. (2019), An efficient architecture to ensure data integrity in ERP systems, 5th International Conference on Advanced Computing & Communication Systems, pp. 236-241, DOI: 978-1-5386-9533-3/19/\$31.00
11. Popescu, C.R., Popescu, G. (2018), Risks of cyber attacks on financial audit activity, *Audit Financiar*, vol. XVI, nr. 1 (149) / 2018, pp. 140-147, DOI: <10.20869/AUDITF/2018/149/006>
12. Rădulescu, M.C. (2016), Considerations on the selection and prioritization of information security

- solutions, *Audit Financiar*, vol. XIV, nr. 5 (137)/2016, pp. 564-574, DOI: 10.20869/AUDITF/2016/137/564
13. Rîndașu, S.M. (2018), Information security challenges – vulnerabilities brought by ERP applications and cloud platforms, *Audit Financiar*, vol. XVI, nr. 1 (149) / 2018, pp. 131-139, DOI: 10.20869/AUDITF/2018/149/005
 14. Rîndașu, S.M. (2019), The Security of Accounting Information – A Perception-Based Analysis of the Practitioners from Romania, *Audit Financiar*, vol. XVII, nr. 2 (154) / 2019, pp. 298-305, DOI: 10.20869/AUDITF/2019/154/012
 15. Senior Software (2020), What is ERP?, available at: https://www.seniorsoftware.ro/erp/ce-inseamna-erp-software-erp-sistem-erp-soft-erp-romania/?gclid=EAIaIQobChMlu_KCr_-W-wIVZI9oCR2tZgyVEAAYASAAEgLVD_D_BwE, accessed on November 10, 2022
 16. Sharma, C., Maheshwari, S. (2014), Ten security practices to a formidable ERP system, *International Conference on Smart Structures & Systems India*, pp. 41-50, DOI: 978-1-4799-6506-9/9
 17. She, W., Thuraisingham, B. (2007), Security of Enterprise Resource Planning Systems, *Information Systems Security*, vol. 16, pp. 152-163, DOI: 10.1080/10658980701401959
 18. Sorheller, V.U., Hovik, E.J., Hustad, E., Vassilakopoulou, P. (2018), Implementing cloud ERP solutions: a review of sociotechnical concerns, *Procedia Computer Science*, vol. 138, pp. 470-477
 19. Weng, F., Hung, M.C. (2014), Competition and challenge on adopting Cloud ERP, *International Journal of Innovation, Management and Technology*, vol. 5, nr. 4, pp. 309-313
 20. Xu, H., Nord, J.H., Brown, N., Nord, G.D. (2002), Data quality issues in implementing an ERP, *Industrial Management & Data Systems*, vol. 102, nr. 1, pp. 47-58, DOI 10.1108/02635570210414668