INNOVATION AND SECURITY: HOW CLOUD MANAGEMENT AND ACCOUNTING ARE SHAPING THE FUTURE

Ana-Rebeca Neagu (Ion)[1*], Laurențiu-Eduard Ion[2], Beatrice -Elena Gore[3], Emil Grătianu[4], Florin Radu[5]
[1)2)3)4)5)] *Valahia University of Târgoviște, Târgoviște, Romania*

Abstract
This paper examines how cloud accounting can contribute to the modernization of management strategies in the field of public order and national security. It analyzes the benefits of this technology in enhancing transparency, accelerating decision-making processes, and improving resource allocation, with a direct impact on the performance and competitiveness of both public and private entities. Cloud-based systems enhance the traceability of operations and provide real-time financial analytics, thereby supporting data-driven decision-making. In the public sector, digitalization is framed as a fundamental condition for institutional accountability and operational security, highlighting the necessity of robust governance and cybersecurity policies. The study also emphasizes the importance of proactive managerial approaches oriented toward prevention, legitimacy, and effective conflict management. To strengthen the theoretical framework, the paper proposes a conceptual case study illustrating how a public security institution could integrate cloud accounting solutions to improve transparency, financial control, and strategic resource allocation. This perspective supports the authors' hypothesis that cloud technologies can simultaneously enhance economic performance and national security within an integrated managerial framework grounded in efficiency, coordination, and cybersecurity compliance.

Keywords
accounting, Cloud, strategic management, national security, transparency

JEL Classification
M41, M15, H56, H83, O33

Introduction

The digitization of public administration in Romania represents not only a modernization objective but also a fundamental condition for enhancing efficiency, transparency, and institutional accountability. However, for institutions responsible for security and public

[*] Corresponding author, **Ana-Rebeca Neagu (Ion)** – rebecaneagu@yahoo.com

order, the adoption of cloud technologies is accompanied by the imperative of ensuring the integrity, confidentiality, and resilience of information systems.

In Romania, the availability of cloud ERP and accounting solutions has been examined in the literature, with studies indicating a relatively low adoption rate among companies, primarily due to infrastructure limitations, data security concerns, and organizational resistance to change (Gheorghiu, 2024). Although these studies focus predominantly on the commercial sector, they provide a relevant empirical foundation for understanding the technological, cultural, and regulatory barriers characterizing the Romanian environment.

In the field of managerial accounting, recent research conducted in Romania demonstrates that the integration of digital technologies, including cloud computing and advanced analytics, can optimize costs, improve decision-making processes, and enhance competitiveness, even in organizations with limited resources, provided that clear strategic planning and adequate human resource development are ensured (Pantea et al., 2024).

At both theoretical and applied levels, the literature on digital governance and accounting systems supports the view that digital transformation—particularly migration to cloud infrastructures—can strengthen financial transparency and public accountability, provided that robust data governance and cybersecurity frameworks are implemented (Androniceanu, 2021; Matei & Săvulescu, 2022; Pavlović et al., 2023). This dynamic is especially relevant for security and law enforcement institutions, where vulnerabilities in cloud architectures may generate systemic risks.

Within the European context, strategic initiatives encouraging Member States to adopt "Cloud-First" or sovereign cloud approaches in public administration further underscore the importance of ensuring data sovereignty and institutional trust in digital public systems (Calcara, 2025). The intersection between cloud computing and security is therefore not merely a technological concern, but a central component of broader digital sovereignty strategies.

Unlike the existing literature, which predominantly examines cloud accounting in commercial organizations or private sector contexts, the present study advances an integrated approach tailored to public security institutions. The novelty of this research lies in combining bibliometric analysis with a conceptual model adapted to the institutional and regulatory specificity of the public order sector, emphasizing the interdependence between financial management, digital governance, and cybersecurity. In doing so, the article extends the current theoretical framework by demonstrating the transferability of cloud adoption models to sectors characterized by heightened security requirements, accountability obligations, and European compliance constraints.

Against this theoretical and empirical background, the central research question guiding this study is: to what extent can cloud accounting be integrated into the managerial and accounting strategies of security institutions in Romania in order to simultaneously enhance performance, transparency, and national security?

The following sections present the conceptual framework adapted to the Romanian context, analyze the advantages and risks associated with implementing cloud accounting in sensitive public institutions, and illustrate—through a conceptual case study—how a security institution could adopt a cloud accounting system to improve traceability, financial control, and strategic resource allocation

1. Review of the scientific literature

Cloud computing has emerged as one of the most transformative technologies of the past decade, fundamentally reshaping how organizations manage data, processes, and decision-making systems. In accounting, the transition from on-premise infrastructures to cloud-based solutions has enabled greater operational flexibility, real-time access to financial information, and reduced IT infrastructure costs. Key advantages include the automation of financial workflows, seamless integration with ERP modules, and the application of advanced analytics to accounting data.

In Romania, cloud accounting has been adopted primarily in the private sector, particularly among small and medium-sized enterprises (SMEs), where cost efficiency and technological accessibility serve as major drivers (Ionescu, 2023). Nevertheless, significant expansion potential exists within public administration, especially in the context of digitalization initiatives financed through the National Recovery and Resilience Plan (PNRR) and Government Decision no. 112/2023, which requires public sector applications to be developed as "cloud-ready" or "cloud-native."

At the European level, comparative analyses indicate that countries such as Estonia and Poland have implemented digital accounting solutions at the central government level, achieving measurable reductions in bureaucracy and improvements in financial transparency (Pavlović et al., 2023). Romania currently occupies an intermediate stage of digital transformation, marked by the implementation of the Government Cloud project coordinated by the Authority for Digitization of Romania, designed to provide a unified infrastructure for digital public services.

Both academic research and European institutional practices demonstrate that cloud accounting represents not merely a technological innovation, but a catalyst for organizational transformation, with direct implications for efficiency, transparency, and governance within public institutions.

Public institutions with security responsibilities—such as the Romanian Police or the General Inspectorate for Emergency Situations—are under continuous pressure to modernize managerial practices and ensure the transparent and efficient use of public resources. The literature consistently emphasizes that the digitalization of administrative processes is a prerequisite for institutional accountability and legitimacy, particularly in a context where citizens demand greater access to information and oversight of public expenditure (Androniceanu, 2021).

Cybersecurity plays a pivotal role in this transformation, being framed not only as a technical requirement but as a strategic dimension of governance. Within the European Union, regulatory frameworks such as the NIS2 Directive and the GDPR establish comprehensive standards for protecting data and critical infrastructures. Romania has transposed these regulations through GEO no. 155/2024, thereby reinforcing public institutions' obligations regarding IT security. Concurrently, the National Cybersecurity Strategy (2022–2027) identifies public administration as a priority domain for protection.

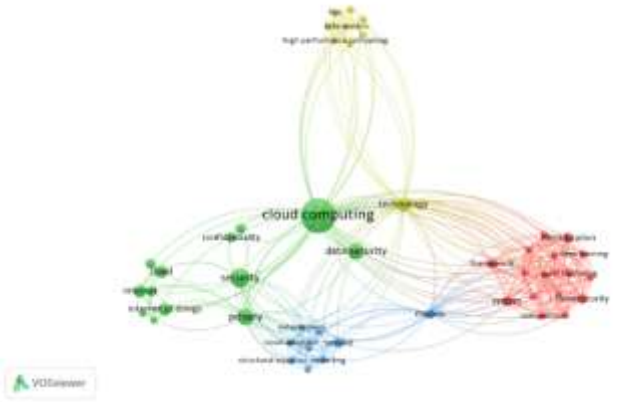
Compared with other EU Member States, Romania continues to face structural challenges, including limited interoperability between information systems, bureaucratic inertia, and constrained financial resources allocated to digitalization (Matei & Săvulescu, 2022). However, recent progress in implementing the Government Cloud platform and

launching pilot digitalization projects—such as those targeting health and education resource management—suggests gradual convergence with European best practices.

For security institutions, the stakes of digital transformation are twofold: the adoption of advanced financial management tools that facilitate rapid decision-making and efficient resource allocation, and the safeguarding of sensitive data and critical infrastructures against cyber threats. This dual imperative explains the growing interest in cloud accounting solutions, which have the potential to reconcile operational efficiency with enhanced security standards.

To capture recent developments in the research landscape, a bibliometric analysis of publications indexed between 2015 and 2025 was conducted. The findings reveal that cloud computing constitutes the central conceptual node in the literature, around which three major thematic clusters have emerged (see Figure no. 1).

Figure no. 1. Cloud computing and dominant clusters



Source: Personal creation, using the VOSviewer program

The main findings of the bibliometric analysis are summarized below:

- Green cluster – Security and privacy: This cluster encompasses terms such as security, privacy, confidentiality, data security, and Internet of Things. It reflects the persistent concern for data protection and information governance in cloud environments, as well as the emphasis on user trust, regulatory compliance, and institutional accountability.
- Blue cluster – Models and adoption: This cluster includes terms such as models, services, determinants, cloud adoption, and structural equation modeling. It indicates a strong research orientation toward identifying the determinants of cloud adoption and evaluating its impact on organizational performance through quantitative methodologies.
- Red cluster – Cybersecurity and artificial intelligence: This cluster brings together terms such as cybersecurity, deep learning, identification, and framework, highlighting an emerging research direction focused on integrating cloud computing with artificial intelligence solutions and enhancing the protection of critical infrastructures.

The chronological analysis reveals a three-stage evolution of the field:

- 2015–2018: Research concentrated primarily on security and privacy concerns, reflecting institutional reluctance and distrust regarding the outsourcing of sensitive data to cloud infrastructures.
- 2018–2020: The focus shifted toward adoption models and organizational determinants, with increased use of quantitative approaches (e.g., SEM) to assess economic and performance-related implications.
- 2021–2025: The field entered a maturation phase characterized by the integration of cloud technologies with cybersecurity and artificial intelligence, alongside the development of conceptual frameworks aimed at protecting critical infrastructures and enhancing digital resilience.

The collaboration network illustrated in Figure no. 2 reveals a densely interconnected scientific community marked by interdisciplinarity and extensive international cooperation. This pattern confirms that research on cloud computing and security is widely distributed across institutions and regions, rather than concentrated within a limited number of academic centers.

Figure no. 2. Interconnecting the scientific community

Source: Personal creation, using the VOSviewer program

The bibliometric analysis identifies three major evolutionary trajectories within the field. First, security and privacy remain central concerns in the literature; however, they are no longer addressed solely from a technical standpoint. Instead, they are increasingly embedded within broader discussions on public policy, institutional governance, and digital sovereignty, reflecting the maturation of the field and the recognition of its strategic relevance.

Second, recent studies emphasize the growing importance of adoption models in explaining the diffusion of cloud solutions across both private and public sectors. Determinants such as cost structures, technological infrastructure, regulatory frameworks, and digital competencies are shown to significantly influence implementation outcomes and organizational performance.

Third, the integration of cloud computing with artificial intelligence and advanced cybersecurity mechanisms signals a new stage of research development. This phase is characterized by the emergence of intelligent, proactive solutions designed not only to enhance operational efficiency but also to strengthen the protection of critical infrastructures and institutional resilience.

Overall, the bibliometric findings demonstrate a clear convergence between transparency, managerial innovation, and security imperatives. This convergence provides a robust theoretical foundation for the subsequent case study applied to the General Inspectorate of the Romanian Police, where these dimensions intersect within a public security context.

2. Research methodology

This paper has a mixed methodological design, combining a bibliometric analysis with an applied case study. This dual approach aims to provide both an overview of research trends in cloud accounting and information security, as well as an applied perspective, relevant for public institutions in Romania.

The first stage consisted of bibliometric analysis, used to identify the thematic evolution, the structure of the research network and the main conceptual clusters associated with cloud computing, digital accounting and cybersecurity. The results of this analysis provide the theoretical foundation for the applicative part of the article.

The second stage consisted of the development of a hypothetical case study applied to the General Inspectorate of the Romanian Police (IGPR). This study was designed based on official documents, strategic reports and relevant national and European legislation, to illustrate how cloud accounting could be implemented in a public security institution, highlighting the associated benefits and challenges.

The main international scientific databases, especially Scopus and Web of Science, were used to carry out the bibliometric analysis, targeting publications published between 2015 and 2023. The documentation process involved queries based on relevant keyword combinations, such as cloud computing, cloud accounting, cybersecurity, public management, and security institutions. In order to ensure the relevance and rigor of the selection, specific filters were applied, through which only scientific articles and papers presented at conferences were retained, with a direct impact on the fields of digital accounting, organizational management and institutional security.

The processing and visualization of the bibliometric data was carried out with the help of the VOSviewer software (version 1.6.19), which allowed the generation of networks of co-occurrence of keywords and collaborations between authors.

For the case study on the General Inspectorate of the Romanian Police, the data sources included:

- official documents of the institution (activity reports, strategies published on the IGPR website);
- the relevant national legislation (Government Decision no. 112/2023 on the government cloud, GEO no. 155/2024 on cybersecurity, National Cybersecurity Strategy 2022–2027);
- European documents (NIS2 Directive, GDPR);
- recent specialized literature, useful for building the applied scenario and for substantiating the benefits and risks of cloud accounting.

By combining these sources and tools, the article aims to provide a rigorous and well-contextualized analysis that reflects both theoretical perspectives and the practical applicability of cloud accounting in public security institutions.

The research presents a number of methodological limitations that must be taken into account in the interpretation of the results. First of all, the case study used is mainly conceptual and hypothetical, not being supported by real institutional financial data, for privacy and security reasons. Secondly, the analysis does not include empirical validation by quantitative methods (questionnaires, SEM models or administrative data), which limits the possibility of generalising the conclusions. Consequently, the results should be interpreted as an analytical and exploratory framework, meant to inform future empirical research.

3. Results and discussion

Case Study: IGPR and Cloud Accounting

The General Inspectorate of the Romanian Police (IGPR), as a central authority responsible for maintaining public order and safeguarding national security, faces multiple managerial and operational challenges that constrain organizational efficiency. Among the most significant are bureaucratic inertia, limited traceability of expenditures, delays in accessing consolidated financial data, and difficulties in the optimal allocation of resources. These structural constraints contribute to institutional rigidity and diminish the IGPR's capacity to respond rapidly and effectively to crisis situations.

Within this context, the implementation of a cloud accounting system represents an innovative strategic solution capable of simultaneously enhancing transparency and managerial efficiency while strengthening cybersecurity and institutional accountability. The proposed modernization framework involves the development of a secure cloud-based platform integrating automated financial reporting, digital auditing mechanisms, and predictive analytics tools. This platform would be interconnected with existing human resources and logistics systems, enabling a comprehensive and real-time overview of institutional resources and supporting more efficient planning of expenditures and strategic investments. This modernization model is illustrated in Figure no. 3, which highlights how the digitization of financial processes leads to operational efficiency and improved performance.

Figure no. 3. Digital transformation of financial processes through Cloud accounting

Source: Personal Creation

To ensure a high level of protection, the platform would be governed by strict cybersecurity and data governance policies, including end-to-end encryption, multi-factor authentication, and real-time access monitoring. This architecture would allow not only the security of financial flows, but also compliance with the European standards imposed by the GDPR and the NIS2 Directive, recently transposed into national legislation.

A concrete example of the application of this model can be seen in the event of a security crisis, such as a wave of protests or a natural disaster, which requires the rapid redistribution of additional funds for the mobilization of personnel, equipment and logistical resources. Currently, in the traditional system, budget allocation procedures often take days or even weeks, due to the bureaucratic cycle and the lack of consolidated real-time data.

By implementing cloud accounting, the decision-making flow would be digitized and integrated, allowing the necessary funds to be allocated in a matter of hours. This speed of reaction would increase the capacity of the IGPR to manage critical situations, reducing the risks associated with operational delays.

The adoption of cloud accounting within the IGPR would have a multidimensional impact. At the operational level, the processing time of financial flows could be reduced by up to 50%, which would allow for a more efficient use of resources. At a strategic level, access to real-time financial data would support evidence-based decision-making, strengthening the institution's managerial capacity. From an institutional perspective, such a system would increase transparency and accountability, helping to increase public legitimacy and strengthen citizens' trust. Finally, on the security dimension, implementing rigorous standards for the governance and protection of sensitive data would reduce cyber vulnerabilities and provide a more resilient infrastructure for managing critical information.

The IGPR case study demonstrates that cloud accounting should not be regarded merely as a supportive technological instrument, but rather as a driver of institutional transformation. The insights derived from this analysis may be extended to other public security institutions in Romania, emphasizing that digital modernization of financial

management systems contributes to the development of more efficient governance frameworks, the reduction of bureaucratic constraints, and the strengthening of cybersecurity resilience. In this regard, the IGPR may serve as a pilot model for cloud integration within the public sector, with tangible implications for operational performance and national security.
To synthesize the manner in which cloud accounting can address the institutional challenges identified within the IGPR, Table no. 1 outlines the key relationships between existing structural problems, the proposed cloud-based solutions, and their anticipated organizational impact.

Table no. 1. Summary of the identified challenges and benefits of Cloud accounting for the General Inspectorate of the Romanian Police

Challenges identified	Solutions proposed through Cloud accounting	Anticipated impact
Excessive bureaucracy and slow procedures	Digitization of financial flows and integration into a single platform	Reduce processing time by up to 50%
Lack of traceability of expenses	Automated financial reporting and digital audit	Increasing transparency and institutional accountability
Delay in obtaining financial data	Real-time access to predictive data and analytics	Quick decisions based on up-to-date data
Difficulties in allocating resources	Platform integration with HR and logistics	More efficient use of available resources
Cyber vulnerabilities	Strict security policies (end-to-end encryption, MFA, data governance)	Strengthening the protection of sensitive information and reducing cyber risks

Source: In-house processing

Therefore, the implementation of Cloud accounting at the IGPR level is not only a technological solution, but a strategic tool for institutional modernization, capable of ensuring transparency, efficiency and a higher level of security in the management of public resources.
The results obtained from the bibliometric analysis and the case study applied to the IGPR confirm the hypothesis that Cloud accounting is a tool for organizational transformation with simultaneous effects on managerial efficiency, institutional transparency and national security.
The bibliometric analysis highlighted the existence of three major clusters in the recent literature: security and privacy, adoption models, and integration with AI and cybersecurity. These directions confirm the maturation of the field and the shift from defensive concerns to proactive approaches. At the same time, studies on digital accounting show that the benefits of cloud deployment go beyond the operational dimension, expanding to the strategic and institutional level.

In the figure below (see Figure 4), we can see the three major directions resulting from the bibliometric analysis – security and privacy, adoption models and integration with AI and cybersecurity – reinforcing the theoretical interpretation through a schematic representation of the current technological landscape.

Figure no. 4. The main thematic clusters identified in the specialized literature on Cloud accounting

Source: Personal Creation

In the international literature, cloud adoption is analyzed in relation to determining factors such as costs, digital skills or the regulatory framework. The IGPR case study brings a local dimension and shows that in Romania, these benefits are particularly relevant in the context of bureaucratic constraints and pressure for transparency. Thus, what the literature describes as "operational efficiency" translates, in the case of the IGPR, into a reduction in the time of redistribution of resources in large-scale national operations, and what is called "digital governance" materializes in increased public legitimacy.

Examples from other EU countries, such as Estonia or Poland, show that the digitization of public accounting via the cloud has generated tangible results: reduced administrative costs, interoperability of systems and increased institutional accountability (Pavlović et al., 2023). Romania aligns itself with these trends through the Government Cloud project and the transposition of the NIS2 Directive, but implementation in security institutions remains limited. The IGPR case study suggests that there is potential to replicate European best practices, but success depends on managerial will and the development of internal digital skills.

Theoretically, the article confirms that the cloud adoption models discussed in the international literature (determinants, SEM, etc.) can also be adapted to security institutions, not just commercial organisations. Basically, the implementation of Cloud accounting at the IGPR level can be seen as a pilot study for other public security structures (see Figure no. 5), with an impact on:

- (faster and more efficient processes);
- strategic (data-driven decisions);
- institutional (increasing transparency and accountability);

- (protection of sensitive financial data).

Figure no. 5. Dimensions of the impact of cloud accounting in public security institutions

Source: Personal Creation

The paper is based on a bibliometric analysis and a hypothetical case study applied to the IGPR. This approach confirms the relevance of cloud accounting for security institutions, but it cannot capture the full complexity of the actual implementation. Future research could include comparative studies between several Romanian public institutions or empirical analyses on the perception of staff on accounting digitalization.

Conclusions

The present research demonstrates that cloud accounting represents an innovative solution with significant implications for both managerial efficiency and institutional security. The bibliometric analysis confirmed the dominant trends in recent literature, highlighting the centrality of data security and privacy, the relevance of organizational adoption models, and the progressive maturation of the field through integration with artificial intelligence and advanced cybersecurity solutions. These developments underscore the multidimensional character of cloud computing, which extends beyond the scope of a conventional information technology tool and evolves into a strategic framework for governance, resilience, and competitiveness.

Beyond its theoretical contributions, the study offers important implications for decision-makers in the field of public order and institutional security. From a governance

perspective, cloud accounting can function as a strategic instrument for strengthening financial control and enhancing institutional accountability within security organizations. The implementation of secure cloud-based platforms increases the traceability of expenditures, reduces operational risks, and improves decision-making through access to real-time financial data. Simultaneously, the integration of cybersecurity mechanisms and robust data governance policies facilitates compliance with European regulatory frameworks concerning data protection, digital resilience, and information sovereignty. In this context, cloud accounting emerges not merely as a technological solution, but as a catalyst for institutional modernization and administrative legitimacy.

The conceptual case study conducted at the level of the General Inspectorate of the Romanian Police (IGPR) illustrates how the implementation of a cloud accounting system can address persistent challenges such as bureaucratic inefficiencies, limited financial traceability, and suboptimal resource allocation. By digitizing financial processes, integrating accounting systems with other institutional platforms, and adopting stringent data governance standards, the institution could achieve measurable improvements in processing efficiency, transparency, decision-making capacity, and the protection of sensitive information.

Overall, the findings indicate that the adoption of cloud accounting should not be perceived solely as a technological upgrade, but rather as a strategic transformation capable of aligning economic performance objectives with national security imperatives. The results therefore support the working hypothesis that cloud accounting can become a critical instrument for modernizing public sector management and strengthening citizens' trust in public governance.Based on the results obtained, several directions of action and future research can be formulated:

- For public institutions – there is a need to develop clear digital governance policies that support the adoption of cloud accounting. These policies should target both technological infrastructure and human resources training, through digital and cybersecurity training programmes.
- For the IGPR and other security institutions – the gradual implementation of a cloud accounting system, through pilot projects, would allow the testing of the proposed solutions and their adaptation to the national specifics. At the same time, working with accredited providers and complying with international security standards would strengthen the protection of sensitive data.
- For the academic environment – comparative studies between various institutions in the field of public security, both nationally and internationally, are recommended to highlight good practices and substantiate a solid theoretical framework on digitized financial management.
- For future research – it is necessary to deepen the relationship between Cloud accounting and new emerging technologies, such as artificial intelligence, blockchain and predictive analytics, to identify proactive solutions for managing resources and protecting critical infrastructures.

The adoption of cloud accounting should be regarded as a strategic investment capable of generating multiple benefits, including enhanced economic efficiency, improved managerial transparency, and strengthened national security. In this sense, cloud accounting evolves beyond its role as a supportive technological instrument and emerges

as a fundamental pillar of institutional transformation, integrating performance objectives with security imperatives within a modern and sustainable managerial framework.
Overall, the study demonstrates that the implementation of cloud accounting—when aligned with robust cybersecurity standards and comprehensive governance policies—can serve as a cornerstone of digital transformation in public security institutions. At the same time, it opens meaningful avenues for future empirical research and informs evidence-based public policymaking in the fields of digital governance and institutional resilience.

References

[1] Alassuli, A., Thuneibat, N. S., Eltweri, A., Al-Hajaya, K., & Alghraibeh, K. (2025). The impact of accounting digital transformation on financial transparency: Mediating role of good governance. Journal of Risk and Financial Management, 18(5), 272. https://doi.org/10.3390/jrfm18050272
[2] Androniceanu, A. (2021). Digital transformation and transparency in public institutions. Transylvanian Review of Administrative Sciences, 17(64), 5–22. https://doi.org/10.24193/tras.64E.1
[3] Bărcănescu, E. D. (2021). Adoption of cloud accounting in Romania: Opportunities and challenges. Journal of Accounting and Management, 11(3), 45–57
[4] Bebeșelea, M. (2024). Management Accounting in the Digital Era–One Accounting as Cloud Accounting Type. *Management Accounting Conference Proceedings*, DOI:10.31410/LIMEN.2023.8
[5] Botar, C.-F. (2024). Bibliometric Analysis of Cloud Accounting Phenomenon (I). CECCAR Business Review, 5(6), 41–53. DOI:10.37945/cbr.2024.06.05
[6] Botar, C.-F. (2025). Cloud Accounting: Benchmarks Regarding the Bibliometric Analysis and Systematic Literature Review. CECCAR Business Review, 6(8), 2–15. DOI:10.37945/cbr.2025.08.01
[7] Calcara, A. (2025). European cloud computing policy: Failing in Europe to deliver? Journal of European Public Policy, 32(1), 112–130.
[8] I-LISA. (2025). Role of sovereign cloud in public sector digital transformation in Europe. European Union Agency for the Operational Management of Large-Scale IT Systems.
[9] Gheorghiu, A. (2024). Cloud-based accounting services – Market analysis and prospects for the future in Romania. Strategic Management Conference Proceedings.
[10] Ionescu, C. (2023). Cloud computing adoption in Romanian SMEs and perspectives for the public sector. Management and Marketing. Challenges for the Knowledge Society, 18(2), 125–138. https://doi.org/10.2478/mmcks-2023-0012
[11] Matei, L., & Săvulescu, C. (2022). Cybersecurity governance in public administration: Lessons from the EU and Romania. Administrative Sciences, 12(3), 85. https://doi.org/10.3390/admsci12030085
[12] Mohamad, A. (2025). Mapping the intellectual landscape of big data in accounting and finance: A decade of bibliometric analysis (2013–2023). *Journal of Scientometric Research*, *14*(1), 201–220. DOI:10.5530/jscires.20251109

[13] Mona, N. K. (2025). Tracing the Knowledge Landscape of Cloud-based Accounting: Trends, Themes, and Insights from Bibliometric Analysis. Journal of Informatics Education and Research, 5(2), 2664. DOI:10.52783/jier.v5i2.2664
[14] Pantea, M. F., et al. (2024). Optimizing Romanian managerial accounting practices: The role of digital technology. Romanian Journal of Economic Forecasting, 27(1), 55–72.
[15] Pavlović, D., et al. (2023). Barriers to digital transformation in Central and Eastern European public administrations. Government Information Quarterly, 40(2), 101784. https://doi.org/10.1016/j.giq.2022.101784
[16] Saad, M., et al. (2021). Cloud accounting adoption: Determinants and organizational performance implications. Journal of Accounting and Organizational Change, 17(4), 517–535
[17] Sampaio, C. (2025). Digital Transformation in Accounting: A Bibliometric Analysis. Accounting, 13(4), 206. DOI:10.3390/2227-7072-13-4-206 — bibliometric on the digitization of accounting and AI
[18] Shchyrba, A., et al. (2021). Cybersecurity risks of cloud-based accounting information systems. Information and Computer Security, 29(5), 810–828.
[19] Shchyrba, I., Lagovska, O., Demianyshyna, O., & Shebeshten, E. (2024). Regulatory challenges and cybersecurity approaches in cloud-based accounting systems. Journal of Information Systems Engineering and Management, 10(2s).
[20] Soveizi, N., et al. (2022). Cloud adoption in government: A bibliometric and systematic literature review. Government Information Quarterly, 39(4), 101716. https://doi.org/10.1016/j.giq.2022.101716
[21] The Government of Romania. (2022). Romania's cybersecurity strategy for the period 2022–2027.
[22] The Government of Romania. (2023). Decision no. 112 of February 8, 2023 on the approval of the Government Cloud Platform Governance Guide. The Official Gazette no. 118/10.02.2023.
[23] The Government of Romania. (2024). Emergency Ordinance no. 155 of 30 December 2024 on cybersecurity. The Official Gazette no. 1332/31.12.2024.
[24] Vo Van, T., et al. (2025). Cloud accounting: A systematic literature review. Global Knowledge, Memory and Communication, 74(3/4), 217–236. https://doi.org/10.1108/GKMC-04-2024-0246
[25] Xu, L., et al. (2023). Application of cloud accounting in enterprise financial forecasting and decision-making in the era of big data. Applied Mathematics and Nonlinear Sciences, 8(1), 1–15. https://doi.org/10.2478/amns.2023.1.00024