Journal of Information Systems Engineering and Management
2025, 10(2s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Regulatory Challenges and Cybersecurity Approaches in Cloud-Based Accounting Systems

Iryna Shchyrba[1,*], Olena Lagovska[2], Olesia Demianyshyna[3], Zoriana Myronchuk[4], Edina Shebeshten[5]

[1]*Dr, Associate Professor, Department of Financial Control and Audit, West Ukrainian National University, Ternopil, Ukraine; Research Fellow, Nottingham University Business School (NUBS), Nottingham, United Kingdom*

[2]*Doctor of Economic Sciences, Professor, Zhytomyr Polytechnic State University, Zhytomyr, Ukraine*

[3]*PhD (Economics), Associate Professor, Department of Finance, Accounting and Economic Security, Pavlo Tychyna Uman State Pedagogical University, Uman, Ukraine*

[4]*PhD in Economics, Associate Professor, The Faculty of Economics, Management and Law, Lviv National Environmental University, Lviv, Ukraine*

[5]*PhD in Economics, Senior Lecturer, Department of Accounting and Auditing, Ferenc Rakoczi II Transcarpathian Hungárián College of Higher Education, Beregszász Transcarpathia, Ukraine*

** Corresponding Author: i.shchyrba@wunu.edu.ua*

ARTICLE INFO

Received: 14 Oct 2024

Revised: 04 Dec 2024

Accepted: 18 Dec 2024

ABSTRACT

Introduction: The article examines the development of cloud-based accounting systems and their regulatory support in 2020–2024. The influence of the latest cloud technologies, Microsoft Azure, Amazon Web Services, and Google Cloud, on accounting automation and financial management is analysed. Current regulatory requirements of the European Union, the United States and the countries of the East Asian region are considered with a focus on data security and risk management.

Objectives: The article aims to identify the impact of regulatory requirements and cybersecurity strategies on developing cloud accounting systems in the corporate sector.

Methods: The research methodology used two groups of methods: theoretical and empirical.

Results: The article analyses how developed countries are tightening their cybersecurity and financial regulation requirements, given the increase in transaction volumes and the number of cyber threats. The main development directions of the cloud accounting systems market for the next five years are identified. The article pays special attention to the role of government agencies in developing regulatory standards for cloud accounting systems. The article highlights the impact of international legislation on the structure of data protection systems, such as AWS and Google Cloud. The strategies of the Financial Conduct Authority in the UK and the Monetary Authority of Singapore, which implement technological requirements for cloud providers to ensure market security and stability, are considered. The article outlines the importance of compliance with international standards for cloud solutions.

Conclusions: Thus, the article highlights the challenges of growing cyber threats amid the growing use of cloud-based platforms for financial data processing. The main cybersecurity strategies based on data encryption and multi-factor authentication are outlined.

Keywords: cloud systems, accounting, regulatory requirements, cybersecurity, financial system, multi-factor authentication, data encryption.

INTRODUCTION

Cloud-based accounting systems have significantly developed in recent years due to the rapid advancement of technology in the financial management of corporate sector projects. In the digital transformation era, companies prefer solutions that ensure automation, business continuity, and business processes are secure. Infrastructure in cloud servers is being actively implemented in accounting systems, providing remote access to financial data and integrating with other corporate systems to a high level of automation of routine processes. The principles of efficient

Copyright © 2024 by Author/s and Licensed by JISEM. This is an open access article distributed under the Creative Commons Attribution License which permitsunrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

processing of large volumes of data and transparency of accounting operations contribute to the productivity of businesses in global trading processes.

Increased legal regulation has responded to the rapid growth in the transactions and data processed by cloud platforms. Government regulators in many countries, such as the European Union through the GDPR and the US Federal Reserve, are implementing strict data security requirements to ensure that cloud systems meet financial and legal standards. These measures are aimed at increasing transparency of operations, protecting confidential data and reducing the risk of financial fraud. In Singapore, the Monetary Authority of Singapore (MAS) implements technological regulations to control the use of cloud systems in the financial sector. The authority also requires providers to comply with security and risk management standards. These measures aim to minimise risks in the global economy at the macroeconomic level.

Cybersecurity of cloud systems has become one of the vectors of global confrontations amid active economic tensions. This is especially evident in the growing number of cyberattacks used as a tool in trade wars. According to [1], the most famous examples are the activities of the United States, China, and the DPRK in conducting such operations. Given the new geopolitical confrontations that states and corporations face, cloud infrastructure is being modernised to protect against cyberattacks and data leaks. Modernisation includes improving traditional security methods, strengthening data encryption and adding multi-factor authentication. At the same time, companies are integrating the latest artificial intelligence technologies for automated threat detection. Large corporations are implementing innovative cyber defence strategies aimed at business continuity, reducing the vulnerability of systems to attacks and mitigating the risks associated with using cloud platforms.

LITERATURE REVIEW

The study of cloud accounting systems and their impact on the corporate sector has become particularly relevant since the early 2020s when technological innovations began to be actively implemented in business processes. According to research by Gou and Deng [2], cloud systems have significantly made it possible to automate accounting processes. As a result, the efficiency of financial data management in large corporations has increased. An essential aspect of such systems is the ability to provide centralised storage and management of financial transactions to reduce the risk of human error. The study by Ria and Susilo [3] emphasises that the transition to cloud platforms has become critical in modernising financial management systems in global corporations. These technologies provide continuous access to data from any device and support scalability.

Another critical issue of the study was strengthening the legal regulation of cloud accounting systems in different countries. As Abdo et al. [4] noted, the growth of data volumes has led to introducing new regulations to protect financial data. The General Data Protection Regulation (GDPR) in the European Union has become one of the most critical initiatives regulating financial information processing and storage in cloud systems. Articles by Laili et al. [5] indicate that the Federal Reserve plays a vital role in regulating these issues in the United States. It sets requirements for risk management when using cloud platforms for financial transactions. The role of these regulations emphasises the global trend towards increased transparency and data security in international business.

The cybersecurity of cloud accounting systems has gained new importance with the increase in cyberattacks worldwide. According to research by Musyaffi et al. [6], the number of attacks on cloud platforms has increased by 30 % over the past three years. This encourages companies to develop new cyber defence strategies. The study by Yin [1] describes how data encryption, multi-factor authentication, and traffic monitoring technologies have become essential for protecting financial data in the face of growing cyberattacks. The author also reveals the role of Salesforce and SAP Cloud platforms, which ensure the protection of confidential information by integrating modern automation methods.

Scholars debate the root causes of the rapid introduction of digital technologies in the financial sector, which is occurring in the global digitalisation trend. As noted by Zheng et al. [7], cloud platforms reduce IT infrastructure costs and improve productivity through automation. The study by Levytska et al. [8] points out the importance of automating most operations in cloud systems to improve financial data analytics. This allows businesses to respond more quickly to changes in the economic environment. According to the article's results by King et al. [9], machine learning technologies are used mainly to predict financial performance and potential opportunities for reducing risks in business.

The issue of legal regulation of cloud accounting systems is central to recent research. The authors Khoruzhy et al. [10] note that states have strengthened legal regulations to protect financial information. In the European Union, the General Data Protection Regulation has become the basis for regulating data storage in cloud systems. The study by Pradesa et al. [11] examines the legal requirements for cloud platforms in other regions implementing cybersecurity strategies. The article also highlights the importance of standardising cybersecurity rules for G7 countries for 2025–2026 to protect international financial transactions [11].

Researchers pay considerable attention to preventing cyberattacks, as their early detection minimises the negative consequences by reliably protecting data. The article by Vagner and Sarakhman [12] emphasises that cloud systems require enhanced control over data access and multi-factor authentication implementation to protect against intruders. Liu [13] examines the impact of introducing the latest encryption systems on improving financial data security. The author notes that innovative cybersecurity solutions based on new tools being actively implemented in 2023–2024 have become vital to protecting cloud platforms from growing threats [13]. Thus, scientific research considers the peculiarities of cloud systems functioning in a dynamic environment, which requires constant monitoring for compliance with the legal norms of regulators.

The article aims to identify the impact of regulatory requirements and cybersecurity strategies on developing cloud accounting systems in the corporate sector. The focus is on analysing modern technological platforms and their impact on the automation of financial processes and data management. The research is based on studying the mechanisms of legal regulation by government agencies in various jurisdictions and their actual contribution to financial data security in cloud systems. The article analyses the elements of cybersecurity strategies designed to counter cyberattacks, their variations and the difficulty of detection in a progressive digital market.

METHODS

The research methodology used two groups of methods: theoretical and empirical. The first group used analysis and synthesis methods to systematise scientific information on the development of cloud accounting systems based on current research by Scopus and others. The synthesis of data from various sources helped to combine information on current cybersecurity trends and regulatory requirements in different countries. The second group included methods of statistical analysis and comparative research, which were used to assess the dynamics of the cloud accounting systems market from 2020 to 2024. A comparison of the effectiveness of different cloud platforms regarding data security and regulatory compliance was carried out.

The research procedure involved identifying the main trends in the development of cloud technologies in accounting and analysing existing data security requirements. In the first stage, we reviewed vital cloud systems, focusing on compliance with international cybersecurity standards. In the second stage, cybersecurity strategies were investigated, including data encryption methods, access control, and threat detection systems. The selection of systems was based on analysing the most common corporate platforms actively used in international business. The transformation of the corporate sector in response to the introduction of cloud systems was assessed through the impact of technology on the automation of accounting processes.

The article analyses how companies have adapted their business models to the new environment and how implementing cloud-based systems has improved financial management efficiency. The study used comparative analysis methods to evaluate different approaches to implementing regulatory requirements in cloud accounting systems in different countries. The comparison included an analysis of the GDPR requirements for the European Union, the US Federal Reserve's regulations, and the Monetary Authority of Singapore's recommendations. This approach helped identify commonalities and differences in cybersecurity and data management approaches. Particular attention was paid to integrating data privacy requirements and cyber threat mitigation strategies.

RESULTS

Cloud-based accounting systems are integrated technology platforms for accessing accounting data and financial transactions online. Etymologically, the term “cloud” comes from the metaphorical image of the Internet as a cloud, which appeared in the 1990s to describe remote access to resources outside the local infrastructure. The epistemological significance of cloud systems lies in a new approach to data management, where the physical location of information is unimportant, and the main focus is on accessibility, mobility and scalability. Cloud accounting solutions are being implemented to automate financial transactions, simplify reporting and reduce IT infrastructure

costs. They offer practical tools for managing cash flows, monitoring expenses and forecasting financial results. These components make them essential in today's dynamic markets and globalised economy.

Cloud-based accounting systems received a significant boost in 2021–2023 as the COVID-19 pandemic accelerated the global adoption of telecommuting and remote business management technologies [14], [15], [16]. Companies have been forced to adapt to new conditions, including the need to quickly access financial data and manage accounting processes from anywhere in the world. Over the years, the cloud market has grown steadily. In 2021, the overall market for cloud accounting systems reached significant volumes, but it was in 2022 that it grew to USD 4.61 billion. In 2023, the market continued to grow, reaching $5.21 billion, demonstrating businesses of all sizes' rapid adoption of cloud-based systems. This is especially true for small and medium-sized businesses, which saw cloud systems as an opportunity to reduce the cost of maintaining their IT infrastructure. Ukrainian systems, which can compete with European and global ones, have also proved immensely popular. For more details, see Table 1.

Table 1. Examples of Ukrainian, European and Global Cloud Accounting Systems, their Advantages and Disadvantages

System name	Region of origin	Advantages	Disadvantages
1C:Enterprise	Ukraine	Localisation for Ukrainian legislation, wide functionality	High cost for small businesses, complexity of implementation
SAP S/4HANA Cloud	Europe (Germany)	Scalability, integration with other systems	High cost of implementation and maintenance
QuickBooks Online	USA	Easy to use, integration with payment systems	Limited opportunities for large companies
Xero	New Zealand	Intuitive interface, multi-currency support	Limited functionality for large enterprises
NetSuite ERP	USA	Scalability support, extensive ERP functionality	High cost, complexity of settings
MEGAPLAN	Ukraine	Support for Ukrainian legislation, integration with CRM	Limited functionality for international companies
Zoho Books	India	Accessibility and support for small businesses	Limited support for large corporations

Source: compiled by the authors

Cloud-based accounting systems are widely used due to their ease of use, access to data from anywhere in the world, and ability to adapt them to business needs quickly. Despite their significant advantages, each system has limitations, which influence companies' decisions to implement them. The issues of regulatory compliance and ensuring an adequate level of cybersecurity are of particular importance, as this affects data protection and the company's financial performance.

Along with the introduction of cloud solutions, the rapid development of digital commerce has played a vital role in increasing the demand for modern business tools. An increase in international online transactions and the growth of small and medium-sized enterprises in the e-commerce sector stimulated demand for automated accounting systems. They supported the rapid exchange of financial data between different countries and regions. From 2021 to 2023, the role of cloud systems in this process increased significantly, as most companies faced the need to manage their extensive business structures effectively. Cloud platforms have solved this problem by increasing the speed of operations. The importance of digital platforms in the global economy in 2023 is also underlined by the fact that e-commerce has become the basis for economic growth in many countries, requiring innovative approaches to managing financial flows. The average cloud accounting systems market growth rate is 13.1 %, as shown in Figure 1.

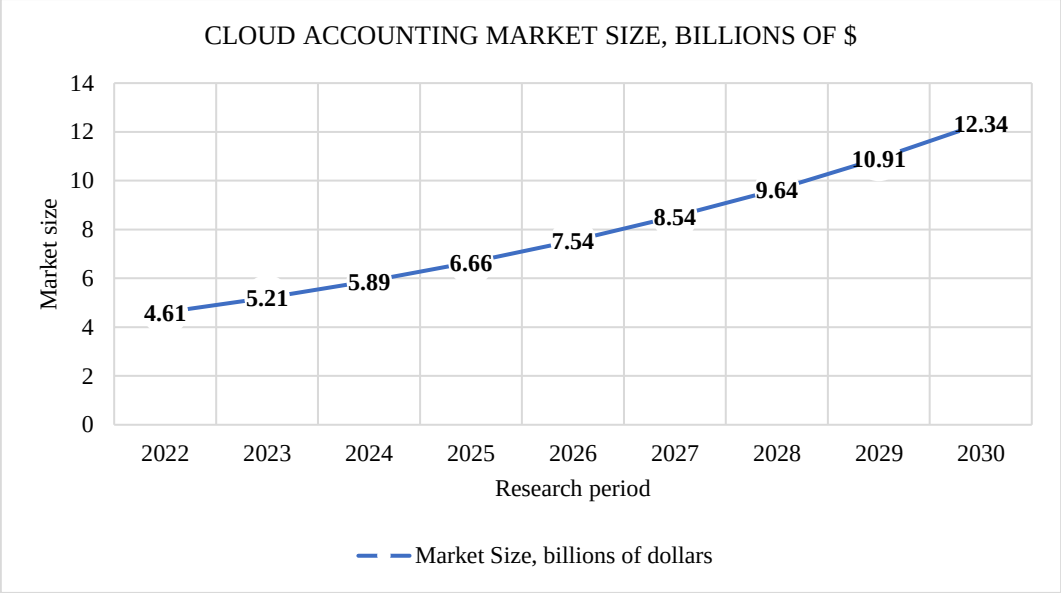

Figure 1. Cloud Accounting Software Market 2023–2030, billion USD

Source: calculated based on [17]

As for the forecasts for the cloud accounting systems market development, the steady growth in the coming years is worth noting. In 2024, the market is expected to reach $5.89 billion; by 2030, it could grow to $12.34 billion. The rapid growth is due to several factors.

Firstly, increased regulatory requirements and growing cyber threats drive businesses to seek solutions to ensure data protection and compliance.

Secondly, more businesses are opting for cloud-based systems because of their flexibility, accessibility, and ability to automate routine processes.

Thirdly, the development of artificial intelligence technologies allows them to be integrated into the APIs of cloud platforms. As a result, it increases the efficiency and security of financial management. In the coming years, the demand for cloud accounting systems will continue to grow, shaping new trends in financial technology.

The practical implementation of regulatory requirements for cloud accounting systems aims to ensure data security and compliance with the laws of various jurisdictions. Regulatory requirements in the US and Europe play a crucial role in protecting personal and financial data. In the United States, agencies such as the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) jointly enforce requirements for managing the risks of third parties, including cloud providers. The European Commission, through the General Data Protection Regulation, sets strict rules for providers like Google Cloud. They relate to the storage and processing of personal data, including the right to be forgotten and the prohibition of data transfers outside the EU. The relevant regulations ensure security and increase transparency of financial transactions, which is critical for companies operating in an international context.

The choice of regulatory authorities and the specifics of their requirements for each cloud system are determined by the specifics of each country's legislation and the scope of the specific platforms. Amazon Web Services (AWS) is guided by the security standards developed by the Cloud Security Alliance (CSA), where the main goal is to ensure transparency and risk management in the financial sector. In the UK, the Financial Conduct Authority (FCA) regulates cloud providers through requirements for outsourcing management in financial institutions, as in the case of Oracle Cloud. The Monetary Authority of Singapore (MAS) implements technology risk management rules that apply to providers in Singapore. Despite the difference in regulatory approaches between countries, the basic principles of data security and risk management remain common [18]. This indicates a global trend towards unifying cybersecurity and data protection standards in cloud systems, as detailed in Table 2.

Table 2. Content of Regulatory Requirements for Cloud Accounting Systems in Different Jurisdictions of the World

System	Regulatory body	Contents
Microsoft Azure	U.S. Federal Banking Agencies (FRB, OCC, FDIC), Joint TPRM Guidance	The joint third-party risk management guidelines require banks to conduct due diligence on cloud service providers and ensure their compliance with banking security requirements.
Amazon Web Services (AWS)	Cloud Security Alliance (CSA), CSA Security, Trust, Assurance Registry (STAR) Programme	Regulates security and transparency practices for cloud providers in the financial sector, including cybersecurity risk management and third-party security due diligence. AWS is certified under the STAR programme.
Google Cloud	European Commission, General Data Protection Regulation (GDPR, Regulation (EU) 2016/679)	Establishes requirements for protecting personal data when storing and processing information in the cloud. There are strict requirements for transparency, the right to be forgotten, and restrictions on data transfers outside the EU.
Oracle Cloud	Financial Conduct Authority (FCA, UK), FCA Handbook SYSC 8	Requirements for outsourcing risk management in financial services, including using cloud providers. The Resolution regulates contingent risk management, including business continuity.
Salesforce	Australian Prudential Regulatory Authority (APRA), APRA CPS 234	Cybersecurity requirements oblige financial institutions to ensure that data is protected and that cloud service providers meet security requirements, including incident management and backup plans.
SAP Cloud	Monetary Authority of Singapore (MAS), Technology Risk Management Guidelines	Managing technology risks associated with using cloud services in the financial sector, including privacy, data security, and service continuity requirements.
Workday	U.S. Department of Treasury, Cloud Services Steering Group	Regulation on managing the risks of concentration of cloud providers in the financial sector. Banks must develop data backup and incident management plans to mitigate business continuity risks.

Source: compiled by the authors

Cyber attacks on cloud accounting systems increased significantly from 2020–2024. The COVID-19 pandemic and the rapid growth of remote work have contributed to increased cyber threats as businesses have massively switched to cloud-based data management platforms. The principal technical vulnerabilities of cloud-based systems include weak access control, poorly configured credentials, and insufficiently secure APIs (application programming interfaces). An incorrect security configuration at Amazon Web Services in 2021 led to the leak of more than 100 million user records. Another critical threat is using stolen or compromised credentials, which accounts for about 30 % of all incidents. Another challenge is the growth of new digital platforms, which are often targeted due to their high value and lack of regulation. According to IBM, in 2023, cyberattacks on cloud platforms reached new heights due to the popularity of new decentralised systems and insufficient security measures on the user side.

The IBM X-Force Threat Intelligence Index 2024 [19] report highlights that a significant portion of cyberattacks on cloud environments in recent years have been related to data storage issues across different cloud environments (public and private). For example, 40 % of incidents are caused by unprotected data stored in different clouds. Such

data can go unnoticed for a long time, increasing the cost of incident response and detection. In 2023, there was a surge in the use of stolen or compromised credentials, which became the most common hacking method, accounting for 30 % of all attacks. This makes cloud services particularly vulnerable to attacks related to mismanagement and misconfiguration, which can lead to the theft of confidential information and significant losses for organisations. The growing reliance on cloud-based solutions in the financial sector increases the importance of implementing multi-layered security. This should include monitoring and access control tools to prevent unauthorised intrusions and ensure compliance with regulatory requirements. The main cyber defence strategies are shown in Figure 2.

Effective cybersecurity strategies for cloud accounting systems start with solid data encryption. Data must be encrypted during storage (data-at-rest) and transmission (data-in-transit). Using AES-256 encryption standards for data on cloud servers and TLS (Transport Layer Security) for data transmission significantly reduces the risk of unauthorised access. Introducing multi-factor authentication adds a layer of protection against credential theft. To improve cybersecurity, it is essential to use automated systems to detect anomalies in traffic, as this allows you to identify suspicious activity and respond to potential threats quickly. Innovative solutions such as SIEM (Security Information and Event Management) allow companies to monitor and analyse real-time events to detect cyberattacks. The size of the cybersecurity market is constantly evolving, as shown in Figure 3, with projected data.

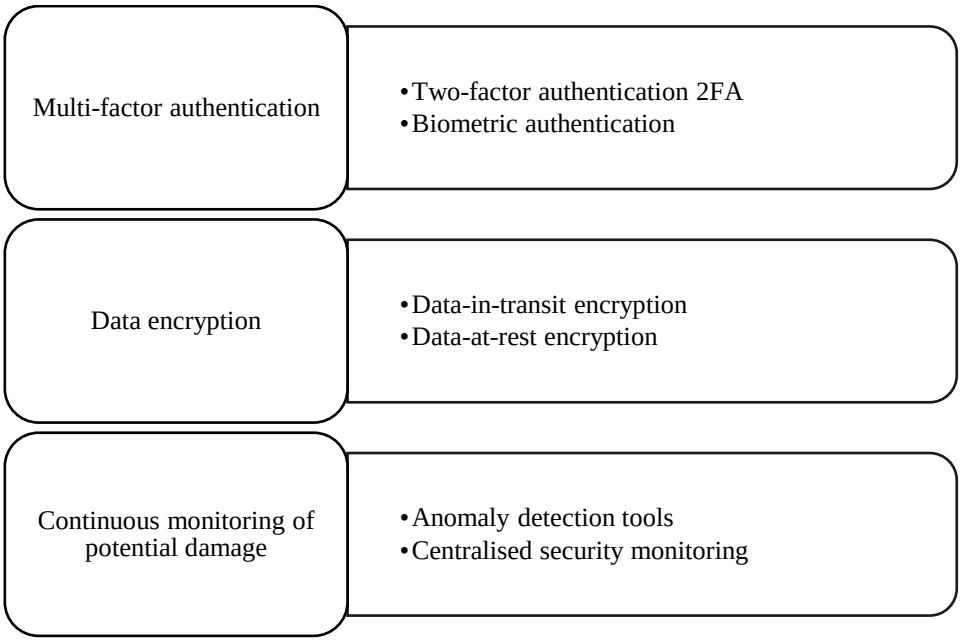

Figure 2. Essential Cyber Security Strategies for Cloud Accounting Systems

Source: compiled by the authors

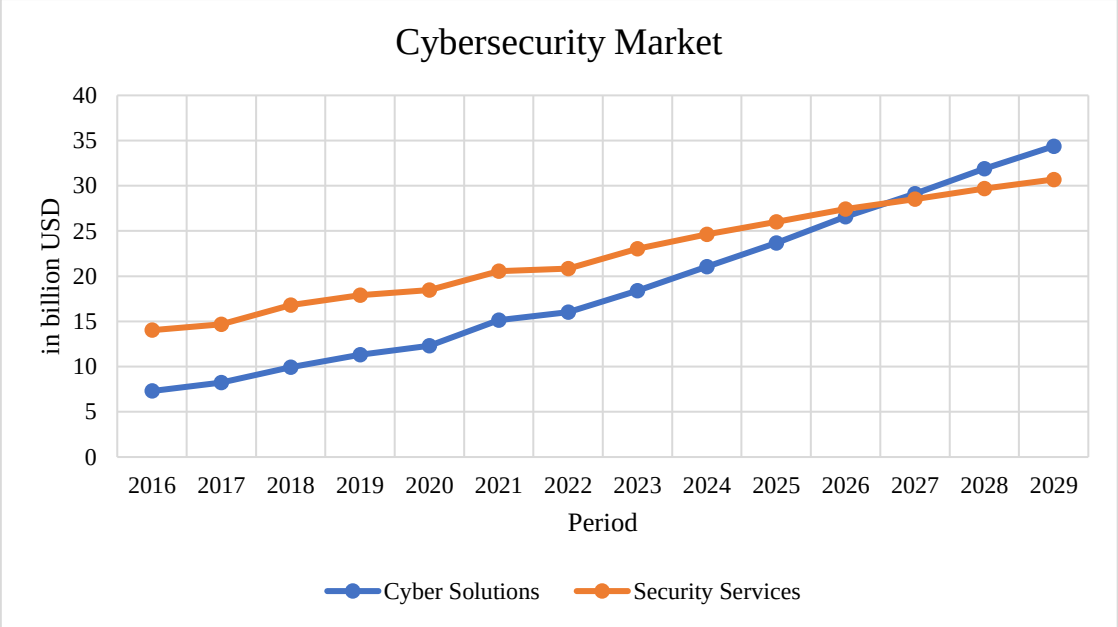

Figure 3. Revenue in the Cybersecurity Market 2016–2029, billion USD

Source: compiled based on Statista [20]

Prospects for developing cloud accounting systems in the next five years are associated with further tightening regulatory requirements and introducing new cybersecurity standards. Europe will continue to implement enhanced personal data protection controls by the GDPR. The regulation provides new requirements for cloud providers regarding data storage and transmission. In the United States, the Federal Reserve and the Office of the Comptroller of the Currency will continue expanding requirements for third-party risk management and verifying cloud providers' compliance with cybersecurity standards. Singapore will tighten requirements through the Monetary Authority of Singapore to create rules to minimise technological risks for cloud systems. We can expect corporations to invest in security by implementing automated risk monitoring and forecasting systems shortly. This approach will become the primary vector of cybersecurity development in cloud accounting systems.

DISCUSSION

The results obtained on the development of cloud accounting systems confirm their importance for automating financial processes in the corporate sector. Our study is in line with Beredugo [21], who emphasises the importance of scalability of cloud platforms for global corporations. Similar to the findings of Abdo et al. [4], we found that integrating AI into cloud accounting systems increases data processing efficiency and allows for better response to changes in the business environment. Comparison with the results of Al Ghatrifi et al. [22] confirms that data encryption and multi-factor authentication are vital measures to protect financial information from cyberattacks. Khoruzhy et al. [10] confirms our findings that government regulations play an essential role in ensuring the security of cloud systems in Europe. We agree with the findings of Japee and Thakker [23], who argues that the number of cyberattacks on cloud platforms has increased significantly over the past three years and that new cybersecurity methods must be implemented. Moron and Diokno [24] analysis demonstrates how government policies influence the development of cloud platforms. This is consistent with our findings on the impact of regulators in the US and Singapore. The study also correlates with the findings of Ukpong [25], who highlights the importance of monitoring traffic in cloud systems to prevent cyberattacks. We agree with the study by Huxley and Brivot [26], which emphasises the need for international coordination to regulate the cybersecurity of cloud platforms effectively. Our results confirm the thesis of Wiyanto [27] that multi-factor authentication is the most effective way to protect credentials in cloud systems. The findings also align with Fahmi et al. [28], who argues that cloud platforms significantly improve productivity and reduce infrastructure costs in large companies. That is why the introduction of cloud-based

accounting systems, combined with effective cybersecurity strategies, is a critical factor in the further development of the corporate sector of the global economy.

CONCLUSION

Thus, the development of cloud-based accounting systems is becoming an integral part of the modern corporate sector, providing automation of financial processes, cost reduction and increased transparency. The introduction of Microsoft Azure, AWS and Google Cloud platforms shows that cloud technologies are becoming vital in managing financial operations on a global scale. Advanced AI, blockchain, and automation solutions allow companies to optimise their work with financial data, which is especially important in a rapidly changing business environment. The tightening of legal regulation in cloud accounting systems indicates the need to ensure adequate data security. To this end, GDPR standards are being implemented in the European Union and the requirements of the Federal Reserve in the United States.

There are prerequisites for developing unified data storage and processing standards at the international level. The lack of harmonisation of standards between countries creates additional challenges for international businesses. Cybersecurity of cloud systems remains a crucial challenge amid the growing number of cyberattacks worldwide. Encryption technologies, multi-factor authentication, and monitoring systems to detect threats help protect data from intruders. The development of cloud platforms will require constant infrastructure upgrades and adaptation to new cyber threats. Companies can implement effective cybersecurity strategies and remain competitive in the global business environment. Further research should focus on cybersecurity strategies to ensure the smooth functioning of companies' financial systems in the coming years.

REFERENCES

[1] Yin, F. Design and Implementation of Financial Accounting System Based on Cloud Computing Technology. In *Proceedings - 2023 Asia-Europe Conference on Electronics, Data Processing and Informatics, ACEDPI 2023*, pp. 58-62. Institute of Electrical and Electronics Engineers Inc, 2023. https://doi.org/10.1109/ACEDPI58926.2023.00018

[2] Gou, C.; Deng, X. A blockchain-based security model for cloud accounting data. *International Journal of Ambient Computing and Intelligence,* 2023, 14(1). https://doi.org/10.4018/IJACI.332860

[3] Ria, R.; Susilo, B. Intensi Penggunaan Teknologi Cloud Accounting Pada Usaha Mikro Kecil dan Menengah (UMKM). *Briliant: Jurnal Riset Dan Konseptual,* 2023, 8(1), 261. https://doi.org/10.28926/briliant.v8i1.1180

[4] Abdo, H.; Owusu, F. B.; Mangena, M. Accounting practices and regulations for extractive industries: a framework for harmonisation. *Journal of Financial Reporting and Accounting,* 2024, 22(1), 147-180. https://doi.org/10.1108/JFRA-07-2023-0425

[5] Laili, N. H.; Khairi, K. F.; Masruki, R. An Analysis of the Use of Accounting System on Cloud: A Case Study in Malaysia. In *Studies in Systems, Decision and Control,* 2023, 470, 999-1010. Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/978-3-031-28314-7_84

[6] Musyaffi, A. M.; Oli, M. C.; Afriadi, B. Drivers of Student Technology Readiness in Using Cloud Accounting to Improve Student Performance. *International Journal of Information and Education Technology,* 2023, 13(8), 1169-1176. https://doi.org/10.18178/ijiet.2023.13.8.1918

[7] Zheng, M.; Huang, R.; Wang, X.; Li, X. Do firms adopting cloud computing technology exhibit higher future performance? A textual analysis approach. *International Review of Financial Analysis,* 2023, 90. https://doi.org/10.1016/j.irfa.2023.102866

[8] Levytska, S.; Pershko, L.; Akimova, L.; Akimov, O.; Havrilenko, K.; Kucherovskii, O. A risk-oriented approach in the system of internal audit of the subjects of financial monitoring. *International Journal of Applied Economics, Finance and Accounting,* 2022, 14(2), 194-206. https://doi.org/10.33094/ijaefa.v14i2.715

[9] King, S.; Agra, R.; Zolyomi, A.; Keith, H.; Nicholson, E.; de Lamo, X.; Brown, C. Using the system of environmental-economic accounting ecosystem accounting for policy: A case study on forest ecosystems. *Environmental Science and Policy,* 2024, 152. https://doi.org/10.1016/j.envsci.2023.103653

[10] Khoruzhy, L. I.; Katkov, Y. N.; Romanova, A. A. Cloud Technologies in the Accounting Information System of Interorganisational Cooperation. In *Innovation, Technology and Knowledge Management*, pp. 25-37, Springer, 2023. https://doi.org/10.1007/978-3-031-13913-0_4

[11] Pradesa, E.; Syahrani, T.; Sakti, R. E. Transformasi Digital Adopsi Software As a Service Layanan Cloud Accounting oleh UMKM. *BUDGETING: Journal of Business, Management and Accounting,* 2023, 5(1), 155-169. https://doi.org/10.31539/budgeting.v5i1.7049

[12] Vagner, I.; Sarakhman, O.; Shurpenkova, R. Analysis of the development of cloud technologies in accounting. *Technology Audit and Production Reserves,* 2023, 4(73), 21-26. https://doi.org/10.15587/2706-5448.2023.289245

[13] Liu, Y. Enterprise Comprehensive Budget Informatisation Management Based on Cloud Accounting and Blockchain Technology. *International Journal on Recent and Innovation Trends in Computing and Communication,* 2023, 11(10), 2489-2498. https://doi.org/10.17762/ijritcc.v11i10.9253

[14] Al-Okaily, M.; Alkhwaldi, A. F.; Abdulmuhsin, A. A.; Alqudah, H.; Al-Okaily, A. Cloud-based accounting information systems usage and its impact on Jordanian SMEs' performance: the post-COVID-19 perspective. *Journal of Financial Reporting and Accounting,* 2023, 21(1), 126-155. https://doi.org/10.1108/JFRA-12-2021-0476

[15] Gyau, E. K.; Owiredu-Ghorman, K.; Amaning, N.; Kpimekuu, P. B. Qualitative Analysis on Costs and Benefits of Adopting a Cloud-Based Accounting Information System: A Case Study of Rural Banks in Ghana. *European Journal of Accounting, Auditing and Finance Research,* 2023, 11(6), 70-91. https://doi.org/10.37745/ejaafr.2013/vol11n67091

[16] Yahiya Bani Ahmad, A.; Hannoon, A.; Ibrahim Al-Daoud, K.; Abu-Alsondos, I. A.; A Al-Qaisieh, M. S. Assessment of Cloud-Based Accounting Technology Adoption and Business Performance. *Kurdish Studies,* 2023, 11(3), 2051-4883. https://www.KurdishStudies.net

[17] Cognitive Market Research. Cloud Accounting Software Market Report 2024 (Global Edition), 2024. https://www.cognitivemarketresearch.com/cloud-accounting-software-market-report#author_details

[18] Oliinyk, O. S.; Shestopalov, R. M.; Zarosylo, V. O.; Stankovic, M. I.; Golubitsky, S. G. Economic security through criminal policies: A comparative study of Western and European approaches. *Revista Cientifica General Jose Maria Cordova,* 2022, 20(38), 265-285. https://doi.org/10.21830/19006586.899

[19] IBM. IBM X-Force Threat Intelligence Index 2024, 2024. https://www.ibm.com/reports/threat-intelligence

[20] Statista. Cybersecurity – Europe. Market Insights Technology, 2024. https://www.statista.com/outlook/tmo/cybersecurity/europe

[21] Beredugo, S. B. Essentials of Cloud Accounting Information System on The Operational Efficiency of Firms In Nigeria. *Journal of Accounting and Taxation,* 2023, 3(2), 123-140. https://doi.org/10.47747/jat.v3i2.1221

[22] Al Ghatrifi, M. O. M.; Al Amairi, J. S. S.; Thottoli, M. M. Surfing the technology wave: An international perspective on enhancing teaching and learning in accounting. *Computers and Education: Artificial Intelligence,* 2023, 4. https://doi.org/10.1016/j.caeai.2023.100144

[23] Japee, G.; Thakker, C. P. Cloud-Based Accounting Technologies: Revolutionising Financial Management. *International Journal of Science, Engineering and Management (IJSEM),* 2023, 10(6), 20-26. https://www.researchgate.net/publication/371946374

[24] Moron, C. E.; Diokno, C. O. B. Level of Readiness and Adoption on the Use of Artificial Intelligence Technologies in the Accounting Profession. *Open Journal of Accounting,* 2023, 12(03), 37-54. https://doi.org/10.4236/ojacct.2023.123004

[25] Ukpong, E. G. Scholastic Analysis of the Impact of Digital Technologies on the Accountancy Profession in Nigeria. *European Journal of Accounting, Auditing and Finance Research,* 2023, 11(6), 41-69. https://doi.org/10.37745/ejaafr.2013/vol11n64169

[26] Huxley, Z.; Brivot, M. On professional destabilisation and accounting self-regulation. *British Accounting Review,* 2024, art. no. 101358. https://doi.org/10.1016/j.bar.2024.101358

[27] Wiyanto, H. Niat Pengunaan Sistem Cloud Accounting di Kalangan UKM di Indonesia: Kerangka Konseptual Model Unified Theory of Acceptance and Use of Technology (UTAUT) yang Dimodifikasi. *Labs: Jurnal Bisnis Dan Manajemen,* 2023, 28(2), 22-26. https://doi.org/10.57134/labs.v28i2.48

[28] Fahmi, M.; Muda, I.; Kesuma, S. A. Digitisation Technologies and Contributions to Companies towards Accounting and Auditing Practices. *International Journal of Social Service and Research,* 2023, 3(3), 639-643. https://doi.org/10.46799/ijssr.v3i3.298