JOURNAL OF ADVANCES IN MANAGEMENT AND BUSINESS INNOVATION

REVIEW ARTICLE
Published Online: July 6, 2026
https://doi.org/10xxxxx/Jambi.2026

Analysis of Information Management System Security in The Utilisation of Information Technology at PT. Bank Central Asia Tbk (BCA)

Meme Sasmita[a] | Ica Quratul Nabila[b] | Gita Aprilia Syafitri[c] | Lia Husniati[d] | Muhammad Ikram[e]

[a,b,c,d,e] Department of Business Administration, Universitas Muhammadiyah Mataram, Indonesia

Abstract

This study aims to analyse the security of Management Information Systems (MIS) in the use of information technology within the banking sector, with a focus on PT Bank Central Asia Tbk (BCA). The method employed is a Systematic Literature Review (SLR), with literature sources obtained from indexing services such as Google Scholar, covering publications from 2016 to 2026. The selection process was conducted systematically through the stages of identification, screening, and evaluation based on pre-defined inclusion and exclusion criteria. The research findings indicate that MIS security in the banking sector has seen significant development through the adoption of technologies such as encryption, firewalls, and artificial intelligence (AI), which are capable of enhancing the detection and mitigation of cyber threats. However, the implementation of these technologies remains partial and has not yet been comprehensively integrated. Furthermore, there is a gap between technical approaches and managerial, governance, and organisational policy aspects, which results in suboptimal security effectiveness. Although the CIA Triad principle remains the primary foundation, empirical evidence within the context of the Indonesian banking sector remains limited. This study emphasises the importance of developing an integrated and contextual security model to enhance the resilience of banking information systems.

Keywords: Information system security, management information systems, banking sector, artificial intelligence

1. Introduction

Advances in information technology in the digital age have driven significant transformation across various industrial sectors, including the banking sector, which is required to adapt rapidly to a dynamic business environment (Ardianto et al., 2024). Digitalisation not only enhances operational efficiency but also expands the reach of services to customers through various electronic channels such as mobile banking and internet banking (Ardianto et al., 2024). In this context, the utilisation of information technology has become a key factor in creating a competitive advantage and improving the quality of banking services. Banks, as financial intermediaries, are required to optimally integrate technology to meet customers' increasingly high expectations regarding the speed, security, and convenience of services (Jureid et al., 2026). This is also reflected in the digital transformation undertaken by PT Bank Central Asia Tbk in delivering various technology-based service innovations. Therefore, digital transformation in the banking sector is no longer an option, but a strategic necessity in the face of global competition (Octaviany et al., 2024).

Management Information Systems (MIS) play a vital role in supporting organisational operations, particularly in the banking sector, which relies heavily on accurate, real-time data management(Mitra et al., 2021). MIS serve as a means of collecting, processing, storing and distributing the information required for managerial decision-making. In the context of modern banking, MIS is not only used to support internal activities but is also integrated with various digital services that enable direct interaction with customers(Mitra et al., 2021). Effective implementation of MIS can enhance operational efficiency, reduce human error, and accelerate business processes. In large banks such as PT Bank Central Asia Tbk, the MIS serves as the backbone for managing financial transactions, risk analysis, and the development of innovative digital services (Yuni, 2025). Consequently, the presence of a reliable and integrated MIS is a crucial factor in supporting the organisation's overall performance(Kurniawan & Nasution, 2026)

As the use of information technology in the banking system increases, information security risks have also risen significantly (Kurniawan & Nasution, 2026). Threats such as cyber attacks, data breaches, phishing, malware, and various other forms of digital crime have become major challenges facing banking institutions. Vulnerabilities in information systems can be exploited by malicious parties to access sensitive data, which could ultimately harm both the institution and its customers (Sari et al.,

 Received: April 1, 2026 | Accepted: Mei 28, 2026

2025). In this context, information system security is a crucial aspect for ensuring the confidentiality, integrity, and availability of data. Major banks such as PT Bank Central Asia Tbk, which handle high transaction volumes and have a broad customer base, are potential targets for cyberattacks (Alfarizi et al., 2024). Therefore, a comprehensive and sustainable security strategy is required to anticipate and mitigate the various risks arising from the use of information technology (Fuji, 2025).

The importance of information system security is a crucial aspect in safeguarding the confidentiality, integrity and availability of data (the CIA triad), particularly given organisations' increasing reliance on digital systems (Jevtić & Alhudaidi, 2023). Confidentiality plays a role in protecting sensitive information from unauthorised access; integrity ensures the accuracy and reliability of data against unauthorised alterations; whilst availability ensures that systems and data can be accessed by authorised parties when required (Radanliev, 2024). Failure to maintain these aspects can lead to serious consequences, such as financial losses due to cyber-attacks, recovery costs, and legal sanctions, as well as reputational damage that impacts declining customer trust and potential business loss (Nurmadani et al., 2026). Therefore, the implementation of effective information security strategies is crucial for mitigating risks and ensuring organisational sustainability. However, there is a view that an excessive focus on security has the potential to hinder innovation due to increased regulation and an overly cautious approach; consequently, a balance is required between strengthening security and technological development in addressing the dynamics of the digital landscape (Le et al., 2025).

Previous research on information system security in the banking sector has identified various technological approaches, such as encryption to protect sensitive customer data and transactions, the use of firewalls to control and monitor network traffic in order to prevent unauthorised access, and the implementation of artificial intelligence (AI)-based security capable of enhancing real-time detection and response to cyber threats (Choithani et al., 2024). Nevertheless, there remains a significant research gap, particularly regarding the scarcity of Systematic Literature Reviews (SLRs) that specifically address the security of Management Information Systems (MIS) in major banks in Indonesia, meaning that understanding of the contextual challenges in this region remains limited (Vasquez Ubaldo et al., 2023). Furthermore, most research tends to focus on the development of conceptual frameworks without being supported by adequate empirical validation, particularly within the context of the Indonesian banking industry (Rani et al., 2026). Therefore, although advancements in security technology continue to progress, the need for comprehensive and context-specific studies remains crucial to strengthen banking security systems holistically (Azizah et al., 2024).

A Systematic Literature Review (SLR) is an essential approach for producing a systematic, transparent and comprehensive synthesis of research, particularly in the field of information security, through the structured process of identifying, evaluating and integrating findings from various studies (Hidayat, 2025). This method is capable of minimising bias whilst enhancing transparency in literature reviews, as emphasised by (Williams Jr et al., 2020),who state that SLRs provide a comprehensive overview of a research topic and strengthen the knowledge base through the synthesis of previous research whilst upholding the principles of transparency and bias reduction. In the context of information security, (Daeli et al., 2026) demonstrated the effectiveness of SLR through a systematic review of the causes of data breaches by identifying 283 articles, which were subsequently selected into 18 main studies based on strict inclusion and exclusion criteria, thereby yielding evidence-based conclusions regarding security system vulnerabilities. Furthermore, Z. (Amin et al., 2022) emphasises that SLR provides a systematic and in-depth approach to obtaining accurate and relevant literature, making it a superior alternative to traditional literature reviews for comprehensively and structurally understanding information security issues.

Based on the findings presented, it can be observed that research on the security of Management Information Systems (MIS) in the banking sector remains dominated by discussions of security technologies such as encryption, firewalls and artificial intelligence, whilst studies that specifically integrate technical, managerial, governance and organisational policy aspects within the context of major banks in Indonesia remain very limited. Furthermore, the majority of research focuses on conceptual frameworks and has not yet provided a comprehensive synthesis regarding the effectiveness of applying the CIA Triad principles in supporting the overall security of MIS. This situation indicates a gap between the development of security technologies and their integrated and contextual implementation within the national banking environment. Therefore, this study aims to analyse the security of the Management Information System in the utilisation of information technology at PT Bank Central Asia Tbk (BCA) through a Systematic Literature Review approach, in order to identify developments in security technology, evaluate the integration between technical and managerial aspects, and formulate a conceptual model that can strengthen the resilience and effectiveness of banking information system security.

2. Materials and Methods

This study aims to comprehensively analyse the security of Management Information Systems (MIS) in the use of information technology, specifically at PT Bank Central Asia Tbk, by identifying various approaches, challenges, and relevant risk mitigation strategies within the context of digital banking. The method employed is a qualitative approach using a Systematic Literature Review (SLR) design to produce a systematic, transparent, and evidence-based synthesis of knowledge. The literature search strategy was conducted in a structured manner through scientific databases such as Google Scholar using relevant keywords, including "information system security", "management information system", "banking security", and

"cybersecurity". The search process was restricted to scientific publications within a specific timeframe (e.g. 2016–2026) to ensure the relevance and recency of the data used.

Next, inclusion and exclusion criteria were established to ensure the quality and relevance of the literature analysed. The inclusion criteria encompassed articles from reputable journals, international conference proceedings, and publications that directly addressed information system security, particularly within the banking sector or technology-based organisations. Meanwhile, exclusion criteria included articles that were irrelevant to the topic, lacked full-text access, or had not undergone a peer-review process. The literature selection process was carried out in stages through the identification, screening, and evaluation of article quality using a systematic approach. Subsequently, the data extraction process was carried out by gathering key information from each selected study, such as the research objectives, methods used, main findings, and recommendations regarding information system security. The collected data was then analysed qualitatively to identify patterns, trends, and research gaps as a basis for formulating the study's conclusions and recommendations.

Figure 1. SIM Security Research Procedure for BCA's Digital Banking Operations

Figure 1. Illustrates that this research procedure begins with the identification of the problem, emphasising the urgency of Management Information System (MIS) security in supporting digital banking operations, particularly at PT Bank Central Asia Tbk, as well as the formulation of objectives to analyse relevant security approaches, risks and strategies. Subsequently, a focused research question (RQ) was formulated to examine the security methods employed, the challenges faced, and the effectiveness of information system security implementation within the banking context. The next stage involved devising a literature search strategy using various scientific databases with specific keywords and a defined publication timeframe to obtain relevant and up-to-date sources. The literature obtained is then screened using inclusion and exclusion criteria to ensure quality and alignment with the research focus. The process continues with the data selection and extraction stage through a phased screening process and the extraction of key information from each selected study, such as methods, results, and findings related to information system security. In the final stage, qualitative data analysis and synthesis were conducted to identify patterns, trends, and research gaps, which were then used as the basis for drawing conclusions and formulating recommendations to strengthen information system security in the use of information technology within the banking sector.

3. Results and Discussion

Based on a synthesis of research findings, several key sub-focus areas can be identified in the study of Management Information System (MIS) security in the banking sector, namely: (1) cyber security technologies (encryption, firewalls, AI), (2) security system integration and implementation limitations, (3) managerial approaches and organisational policies, and (4) the fundamental framework of information security (the CIA Triad and its development model). This categorisation indicates that research is not only focused on technical aspects but is also beginning to evolve towards strategic integration and information security governance.

Tabel 1. Banking MIS Security

No	Field or Focus	Authors' Names	Insights / Research Variables
1.	Cyber Security Technology (Encryption, Firewalls, AI)	Ang et al. (2026); Choithani et al. (2024); Намиот et al. (2022); Amaliyah (2025); Permana et al. (2025)	Increased adoption of encryption, NGFWs and AI; improved threat detection accuracy; MFA as a security control.

No	Field or Focus	Authors' Names	Insights / Research Variables
2.	Security System Integration & Implementation Gaps	Permana et al. (2025); Adzimi et al. (2024); Risyani et al. (2025); Afifah et al. (2025)	The integration of encryption, firewalls and AI remains partial; the effectiveness of these technologies has not yet been fully realised; there are coordination challenges between departments.
3.	Managerial Approaches & Security Policies	Emmanuel et al. (2025); Kayani (2025); Singh (2025); Lohrke & Frownfelter-Lohrke (2026) Hayajneh et al. (2023); Kayani (2025); Hoshmand & Ratnawati (2023); Afifah et al. (2025); Nurmadani et al. (2026)	The gap between technical and managerial aspects; the importance of governance, trust and organisational strategy; the need for a holistic approach.
4.	Security Framework (CIA Triad & Development Model)	Amannah (2024); Ajiga et al. (2024); Harahap et al. (2023); Azizah et al. (2024); Tsabita et al. (2023)	The CIA Triad as a foundation; the implementation of encryption, checksums and backups; the DIE model as a development; the lack of empirical evidence in the banking sector.

Table 1 illustrates that the focus of SIM security research in the banking sector remains dominated by technological aspects, particularly those relating to encryption, firewalls and artificial intelligence. However, there is a significant shift towards broader integration encompassing managerial, policy and organisational governance aspects. Furthermore, although the CIA Triad remains the primary foundation of information security, its implementation in the banking sector still faces various challenges, particularly regarding system integration, coordination between units, and empirical validation. Consequently, the current scope of research points to the need for a more holistic and integrated approach to enhance the overall effectiveness of banking information system security.

3.1 Trends in the Implementation of Information Security in the Banking Sector

The banking sector is increasingly adopting information security technologies such as encryption, firewalls and AI-based intrusion detection systems to counter increasingly complex cyber threats. Encryption serves to protect sensitive data and maintain the confidentiality and integrity of information (Ang et al., 2026), whilst Next-Generation Firewalls (NGFWs) are capable of detecting and blocking complex threats through deep inspection, including of encrypted traffic (Ang et al., 2026; Намиот et al., 2022). Furthermore, AI-based systems enhance threat detection accuracy and reduce false positive rates through large-scale data analysis (Ang et al., 2026; Choithani et al., 2024; Намиот et al., 2022) However, their implementation still faces challenges such as the need for specialist expertise and potential algorithmic vulnerabilities, necessitating the strengthening of comprehensive security strategies.

Research evidence indicates that the adoption of security technologies in the banking sector is increasing, particularly through the implementation of encryption and multi-factor authentication in digital banking (Permana et al., 2025). as well as the trend towards using AI in governance and security(Amaliyah, 2025). However, evidence regarding the comprehensive integration of encryption, firewalls, and AI remains limited; existing studies are generally partial in nature, such as the effectiveness of AI in intrusion detection(Risyani et al., 2025) and the integration of firewalls with IDS (Adzimi et al., 2024). which are not yet specific to the banking sector. Furthermore, there are implementation challenges such as gaps in implementation and coordination between departments within Indonesian banks (Permana et al., 2025), meaning claims regarding integrated AI-based security systems still require further validation.

Research findings indicate that the banking sector has adopted security technologies such as encryption, Next-Generation Firewalls (NGFWs), and AI-based systems, which contribute to enhancing protection against cyber threats (Ang et al., 2026; Choithani et al., 2024; Намиот et al., 2022)However, from an evaluative perspective, their implementation remains partial and has not yet been fully integrated, despite an increase in the use of encryption, multi-factor authentication, and AI in banking security (Amaliyah, 2025; Permana et al., 2025). Existing studies generally only highlight the effectiveness of individual technologies, such as AI-based intrusion detection and the integration of firewalls with IDS, without a unified approach (Adzimi et al., 2024; Risyani et al., 2025). Furthermore, constraints such as limited human resources, potential algorithmic vulnerabilities, and a lack of inter-departmental coordination remain obstacles to optimising system security(Permana et al., 2025).

3.2 The Dominance of Technology-Based Approaches in Cybersecurity

Technology-based approaches to cybersecurity, such as machine learning for anomaly detection, have proven effective with high accuracy (Emmanuel et al., 2025) and improved threat detection in AI-based cloud environments (Kayani, 2025; Singh, 2025). However, there remains a gap in integration with managerial and organisational policy aspects, particularly regarding strategic response and trust management (Emmanuel et al., 2025; Lohrke & Frownfelter-Lohrke, 2026). Therefore, the implementation of cybersecurity requires transparent governance support as well as synergy between technology, human factors, and policy to be more effective and comprehensive (Al Hayajneh et al., 2023; Kayani, 2025).

Research evidence indicates that whilst technical approaches remain dominant in cybersecurity, the need for integration with managerial and policy aspects is increasingly recognised; however, implementation gaps persist (Hoshmand & Ratnawati, 2023; Nurmadani et al., 2026) emphasise the importance of a holistic approach combining technical, governance, and human resource development aspects; yet, empirically, challenges persist in the form of implementation gaps and inter-departmental coordination, despite the adoption of technologies such as MFA and encryption (Afifah et al., 2025).

findings indicate that technology-based approaches such as machine learning and AI are effective in enhancing the detection of cyber threats (Emmanuel et al., 2025; Kayani, 2025; Singh, 2025), yet gaps persist in integration with managerial and policy aspects, particularly regarding strategic response and trust management (Lohrke & Frownfelter-Lohrke, 2026). Although a holistic approach has been emphasised (Hoshmand & Ratnawati, 2023), its implementation remains hampered by a lack of coordination and suboptimal policy implementation, despite the use of technologies such as MFA and encryption (Afifah et al., 2025; Nurmadani et al., 2026)

3.3 The Importance of Implementing the CIA Triad Principle

Information Management System (IMS) security in the banking sector is based on the CIA triad principle, which encompasses confidentiality, integrity and availability in protecting data and systems. Confidentiality is maintained through encryption and access controls to prevent unauthorised access (Fauzi et al., n.d.), integrity ensures data accuracy using techniques such as checksums and digital signatures (AMANNAH, 2024), whilst availability guarantees service access through redundancy and backup mechanisms (Ajiga et al., 2024). Furthermore, new models such as DIE are being developed to enhance the resilience and adaptability of systems to modern security challenges (Ajiga et al., 2024).

Research indicates that the CIA Triad is recognised as the foundation of information security in general, though specific evidence within the banking sector remains limited. (Fauzi et al., n.d.) describe its application in internet banking, whilst (Harahap et al., 2023) emphasise the interdependence of its components. However, empirically, (Azizah et al., 2024) found that implementation and coordination gaps still exist in Indonesian digital banks, and (Tsabita et al., 2023) focused more on security standards without specifically testing the CIA Triad, meaning its role in the success of banking security has not yet been fully confirmed.

Research findings indicate that the CIA Triad remains the foundation of SIM security in banking through the application of encryption, access control, and mechanisms for system integrity and availability (Ajiga et al., 2024; AMANNAH, 2024; Fauzi et al., n.d.). However, from an evaluative perspective, although it is supported conceptually and has begun to be developed using models such as DIE (Ajiga et al., 2024), empirical evidence remains limited, as evidenced by gaps in implementation and coordination (Azizah et al., 2024) and the lack of research specifically testing the CIA Triad within the banking context (Azizah et al., 2024).

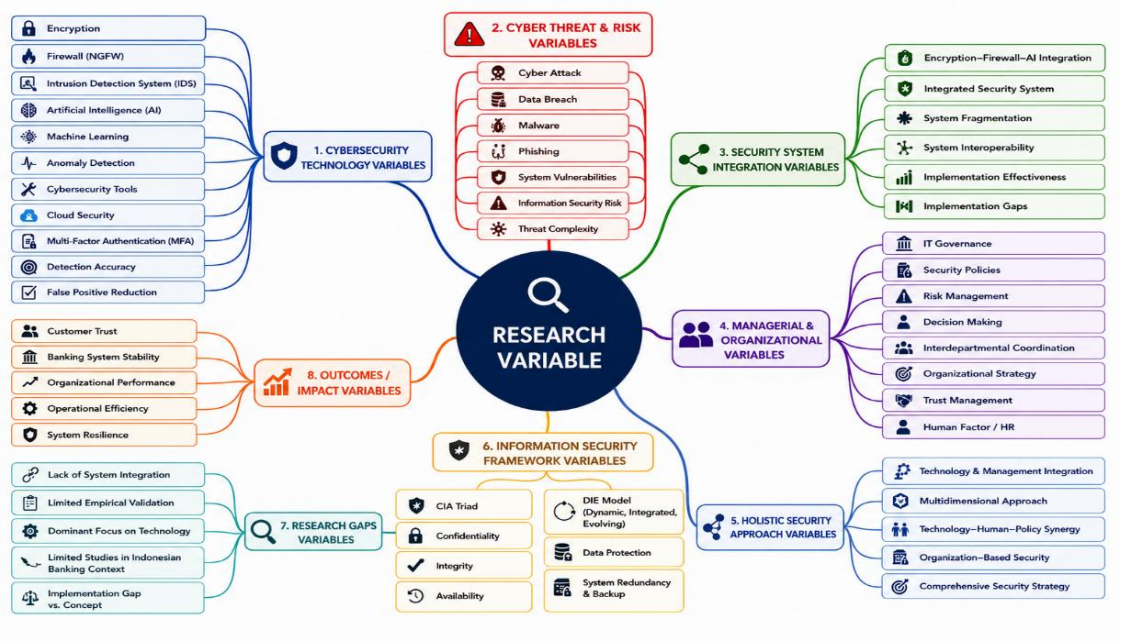

Figure 2. Development of Research Variables in Management Information System Security in the Banking Sector

Figure 2 illustrates the development of research variables in Management Information Systems (MIS) security within the banking sector, covering technological aspects such as encryption, firewalls, AI, IDS and MFA; risk aspects such as cyber attacks, data breaches and malware; security system integration; and managerial aspects such as IT governance, policies and risk management. Furthermore, there are key frameworks such as the CIA Triad and the DIE model, as well as research gaps in the form of a lack of integration and empirical validation, with outcomes including customer trust, operational efficiency, and system resilience, indicating a shift towards a more holistic and integrated approach to security.

4. Conclusions

Based on the evaluation results, it can be concluded that the security of Management Information Systems (MIS) in the banking sector has seen significant progress through the adoption of technologies such as encryption, firewalls and artificial intelligence (AI), which have proven to enhance the ability to detect and mitigate cyber threats; however, their implementation remains largely piecemeal and has not yet been comprehensively integrated. Furthermore, although technology-based approaches dominate, there is a clear gap in integration with managerial, governance, and organisational policy aspects, which impacts the sub-optimal effectiveness of the overall security strategy. On the other hand, the CIA Triad remains the primary conceptual foundation; however, the limited empirical evidence within the banking context, particularly in Indonesia, indicates a gap between theoretical frameworks and practical implementation. Consequently, prominent research gaps include the lack of integration between technology-based security systems and organisational policies, the scarcity of contextual empirical studies, and weak coordination between units in security implementation. Based on these findings, an urgent research topic for future study is the development of an integrated and holistic AI-based banking SIM security model that combines technological, governance, and human factors, accompanied by empirical validation within the Indonesian banking context to produce adaptive, effective, and sustainable security strategies.

Acknowledgment

The author would like to express his deepest gratitude to Muhammadiyah University of Mataram, in particular the Business Administration Programme, for the academic support and facilities provided throughout the course of this research. The author would also like to thank all lecturers, colleagues, and other parties who have provided valuable input and assistance in the completion of this research. This research did not receive any specific funding support from government agencies, commercial entities, or non-profit organisations.

References

Adzimi, S. N., Alfasih, H. A., Ramadhan, F. N. G., Neyman, S. N., & Setiawan, A. (2024). Implementasi konfigurasi firewall dan sistem deteksi intrusi menggunakan Debian. *Journal of Internet and Software Engineering*, *1*(4), 12.

Afifah, E. F. N., Simatangkir, D. W. E., & Faliha, N. S. (2025). Keamanan siber dalam perbankan serta tantangan dan solusi di era

digital. *Jurnal Multidisiplin Ilmu Akademik*, *2*(1), 33–42.
Ajiga, D., Okeleke, P. A., Folorunsho, S. O., & Ezeigweneme, C. (2024). Designing cybersecurity measures for enterprise software applications to protect data integrity. *Computer Science & IT Research Journal*, *5*(8), 1920–1941.
Al Hayajneh, A., Thakur, H. N., & Thakur, K. (2023). The evolution of information security strategies: A comprehensive investigation of infosec risk assessment in the contemporary information era. *Computer and Information Science*, *16*(4), 1.
Alfarizi, R., Satrio, A. J., Praseyto, Y. O., & Syahputra, M. F. (2024). Analisis Perkembangan Teknologi M-Bca Dan Keamanan Siber Di Bank Central Asia. *Jurnal Akademik Ekonomi Dan Manajemen*, *1*(4), 43–53.
Amaliyah, R. (2025). Efektivitas Penggunaan Teknologi Artificial Intelligence Terhadap Proteksi Keamanan Sistem Tata Kelola Perusahaan (Sektor Perbankan). *Info Kripto*, *19*(1), 49–60.
AMANNAH, C. I. (2024). Development and deployment of a security information management system for enhanced organizational safety and efficiency. *International Journal of Convergent and Informatics Science Research*.
Amin, Z. M., Anwar, N., Shoid, M. S. M., & Samuri, S. (2022). Method for conducting Systematic Literature Review (SLR) for cyber risk assessment. *Environment-Behaviour Proceedings Journal*, *7*(SI10), 255–260.
Ang, S., Ho, M., Huy, S., & Janarthanan, M. (2026). A Multi-Layered Adaptive Cybersecurity Framework for the Banking Sector Integrating Next-Gen Firewalls with AI-Driven IDPS. *STAP Journal of Security Risk Management*, *2026*(1), 67–76.
Ardianto, R., Ramdhani, R. F., Dewi, L. O. A., Prabowo, A., Saputri, Y. W., Lestari, A. S., & Hadi, N. (2024). Transformasi digital dan antisipasi perubahan ekonomi global dalam dunia perbankan. *MARAS: Jurnal Penelitian Multidisiplin*, *2*(1), 80–88.
Azizah, S., Ula, Z. N., Mutiara, D., & Prameswari, M. P. (2024). Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile: Studi literatur mengenai cybercrime dan mitigasinya. *Akuntansi Dan Teknologi Informasi*, *17*(2), 221–237.
Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. *Annals of Data Science*, *11*(1), 103–135.
Daeli, I. S., Ningsih, R. S., Limbong, K. L., & Darma, J. (2026). STRATEGI CYBERSECURITY UNTUK PERLINDUNGAN DATA AKUNTANSI: KAJIAN LITERATUR SISTEMATIS 2021-2025. *LAND JOURNAL*, *7*(1), 74–87.
Emmanuel, A., Victor, O. A., Owusu-Afriyie, E., & Ediete, M. A. (2025). AI-Driven Data Privacy and Trust Management in Digital Business Ecosystems: A Machine-Learning Based Framework for Risk Reduction. *2025 22nd International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, 1–5.
Fauzi, A., Fikri, A. W. N., Syukri, A. F., & Dewi, A. (n.d.). *Peran CIA (Confidentiality, Integrity, Availability) pada Layanan Internet Banking di Perbankan*.
Fuji, S. (2025). Strategi Manajemen Risiko Teknol Strategi Manajemen Risiko Teknologi Informasi Berbasis Studi Literatur. *TeIKa*, *15*(1).
Harahap, A. H. H., Andani, C. D., Christie, A., Nurhaliza, D., & Fauzi, A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder. *Jurnal Manajemen Dan Pemasaran Digital*, *1*(2), 73–83.
Hidayat, F. (2025). Peran Teknologi Blockchain, AI, dan ERP dalam Memperkuat Transparansi dan Akuntabilitas Lembaga Sektor Publik Syariah: Sebuah Analisis Literatur Sistematis. *Journal of Economics and Business UBS*, *14*(6), 1510–1529.
Hoshmand, M. O., & Ratnawati, S. (2023). Analisis keamanan infrastruktur teknologi informasi dalam menghadapi ancaman cybersecurity. *Applied Information Technology and Computer Science (AICOMS)*, *2*(2), 9–18.
Jevtić, N., & Alhudaidi, I. (2023). The importance of information security for organizations. *Serbian Journal of Engineering Management*, *8*(2), 48–53.
Jureid, J., Adelina, S., Damayanti, E., Nurhifdah, T., & Mardana, Y. (2026). Tantangan Adopsi Produksi Bank Syariah: Persepsi dan Pengalaman Umat. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *4*(4), 8288–8296.
Kayani, M. A. (2025). AI Driven Cloud Security and Anomaly Detection in Saudi Arabia: A Strategic Enabler of Vision 2030 Digital Transformation (Revised Version–Updated after Peer-Review Feedback, October 2025). *ScienceOpen Preprints*.
Kurniawan, E., & Nasution, M. I. P. (2026). Optimalisasi Sistem Informasi Manajemen Dalam Mendukung Pengambilan Keputusan Organisasi Modern. *Jurnal Ilmu Ekonomi, Pendidikan Dan Teknik*, *3*(1), 91–96.
Le, T. D., Le-Dinh, T., & Uwizeyemungu, S. (2025). Cybersecurity analytics for the enterprise environment: A systematic literature review. *Electronics*, *14*(11), 2252.
Lohrke, F. T., & Frownfelter-Lohrke, C. (2026). Cybersecurity research from a management perspective: A systematic literature review and future research agenda. *Journal of General Management*, *51*(3), 349–360.
Mitra, A. W., PD, A. I. P., Rufaedah, D. S., Santoso, H., & Fahmi, M. S. (2021). Analisis Kebijakan Manajemen Strategis Perbankan dalam Mempersiapkan dan Menghadapi Disrupsi Digital: Studi Kasus pada PT Bank Central Asia Tbk. *Journal of Accounting and Business Studies*, *6*(2).
Nurmadani, S., Ceria, N. A., Khalil, M., Riski, M. F., & Rasyad, M. R. (2026). Keamanan Informasi dalam Sistem Informasi Modern: Analisis Ancaman dan Upaya Pengamanan Berdasarkan Studi Literatur. *JIKUM: Jurnal Ilmu Komputer*, *2*(1), 127–132.
Octaviany, C., Oktavianus, L., & Hasmadi, M. (2024). *Transformasi Digital Ditinjau dari Teori Manajemen Perubahan Lewin:*

Studi Kasus di Bank Digital blu by BCA.

Permana, R. A., Anindita, R., Zainol, Z., & Quinn, A. (2025). Analisis metode dan teknologi untuk perlindungan data dan informasi dari ancaman siber: Analysis of methods and technologies for data and information protection against cyber threats. *Jurnal MENTARI: Manajemen, Pendidikan Dan Teknologi Informasi*, *3*(2), 137–146.

Radanliev, P. (2024). Digital security by design. *Security Journal*, *37*(4), 1640–1679.

Rani, I. H., Widyowati, L. A., & Jalih, J. H. (2026). Agilitas Perbankan dalam Analisis TCCM: Sebuah Tinjauan Literatur Sistematis. *Solusi*, *24*(1).

Risyani, Y., Japit, S., Bombongan, C., Selamat, T., & Yuliana, Y. (2025). Sistem Keamanan Siber Adaptif Berbasis AI: Analisis Kinerja, Arsitektur, dan Penerapannya pada Organisasi Modern. *Jurnal Minfo Polgan*, *14*(2), 2999–3006.

Sari, R. D. N. I., Istan, M., & Hendrianto, H. (2025). *Pengaruh transformasi sistem keamanan dan penggunaan teknologi baru terhadap serangan siber pada data nasabah*. Institut Agama Islam Negeri (IAIN) Curup.

Singh, H. (2025). Enhancing cloud security posture with AI-driven threat detection and response mechanisms. *Available at SSRN 5267878*.

Tsabita, A. W. Z., Fanfa, H. S., & Syahada, M. R. (2023). Systematic Literature Review (SLR): Standar Manajemen Keamanan Sistem Perbankan. *Journal Central Publisher*, *1*(4), 310–327.

Vasquez Ubaldo, A. L., Gutierrez Barreto, V. Y., Berrios Albines, J. A., Andrade-Arenas, L., & Bellido-García, R. S. (2023). *Information security in the banking sector: A systematic literature review on current trends, issues, and challenges*.

Williams Jr, R. I., Smith, A., R Aaron, J., C Manley, S., & C McDowell, W. (2020). Small business strategic management practices and performance: A configurational approach. *Economic Research-Ekonomska Istraživanja*, *33*(1), 2378–2396.

Yuni, A. (2025). Implementasi MIS (Sistem Informasi Manajemen) untuk Meningkatka Efisiensi dan Keamanan Transaksi Antar Bank Menggunakan BCA Mobil: Studi Kasus di Bank BCA Tbk. *Jurnal Cemerlang Ekonomi, Manajemen, Akuntansi Dan Bisnis*, *1*(1), 24–30.

Намиот, Д. Е., Ильюшин, Е. А., & Чижов, И. В. (2022). Искусственный интеллект и кибербезопасность. *International Journal of Open Information Technologies*, *10*(9), 135–147.