

Blockchain and Data Security Management in Financial Services: A Strategic Evaluation with the COBIT 2019 Framework

Desinta Riski Azhari ^{1*}, Khusnul Khotimah ², Samuel Domatius Surya Putra ³, Adz Dzukran Zaki Zharauri Naimullah Shalih ⁴, Angga Rafael Cristian Tambun ⁵, Meisyanda Adelia Rahma Putri ⁶, Jessica Joylynn Kaligis ⁷

¹Department of Digital Business, Surabaya State University Ketintang, Surabaya, 60231, Indonesia
jdbmi@unesa.ac.id

Abstract

In the digital era, data security is a top priority for the banking industry, given the increasing cyber threats and the demands of strict regulatory compliance. This study aims to analyze the impact of blockchain on data security, regulation, and business efficiency in the banking sector, and provide strategic recommendations for companies that want to adopt this technology. The method used is the Systematic Literature Review (SLR) with the PRISMA approach and bibliometric analysis using Publish or Perish and VOSviewer to identify research trends from 2015 to 2025. The case study at Bank XYZ emphasizes the importance of using the COBIT 2019 framework in evaluating and improving IT infrastructure, as well as the need for better risk management and increased collaboration between teams to achieve higher effectiveness. The results of the study show that blockchain technology, IT governance, and cybersecurity are the main pillars in the digital transformation of banking, where the integration of the three can improve efficiency, security, and transparency in digital financial services, although challenges such as cyber threats, regulation, and risk management still need to be overcome to achieve sustainable optimization. However, challenges such as implementation complexity, high costs, and dynamic regulatory changes are still major obstacles. Therefore, this study recommends the implementation of risk-based security strategies, increasing cyber awareness in the workplace, and utilizing cutting-edge technologies such as artificial intelligence (AI) in data protection systems. With a more adaptive approach, banks can strengthen their security systems and minimize potential cyber threats.

To cite this document:

Azhari, Desinta Rizki, Khotimah Khusnul., Putra, Samuel Domatius Surya,m Shalih, Adz Dzukran Zaki Zharauri., Tambun, Angga Rafael Christian., Putri, Meisyanda Adelia Rahma, Kaligis, Jessica Joylynn. (2026). *JDBIM (Journal of Digital Business and Innovation Management, Vol 5. No. 1, 189-208. DOI: 10.26740/jdbim.v5i1.67033*

Keywords: Data Security Management; Banking and Financial Services; Blockchain; Cybersecurity Risk; IT Governance.

Received: xx xxx xxx; Accepted: xx xxx xxx; Published: xx xxx xxx

*Corresponding author

Email: khusnul23504@mhs.unesa.ac.id

INTRODUCTION

Blockchain technology has become one of the most significant advances in various fields, especially in finance and information technology, in the rapidly evolving digital era. To record transactions without the need for intermediaries, blockchain offers a secure, transparent, and decentralized system (ISACA, 2017). It is not only the financial system that uses this technology, but also smart contracts, logistics, and AI (MDPI, 2021). However, the application of this technology still faces many problems, such as scalability, security, and regulation (Zohar, 2015).

Previous research has shown both advantages and disadvantages of blockchain implementation. For example, research on smart contracts shows that while the technology has the ability to improve business efficiency and automate transactions, potential security hazards and legal uncertainty remain a challenge (ISACA, 2022)., in the digital banking sector, the use of bots and artificial intelligence-based technologies has improved operational efficiency, but also raised questions regarding trust and security of customer data (ISACA, 2021a)., studies on technology-based trust show that while blockchain can increase transparency, its implementation requires a deep understanding of security and regulatory aspects (ISACA, 2021b; Nakamoto, 2008).

Digital payment systems, credit, and other financial services have been significantly transformed by blockchain in the banking industry. For example, research by Swan (2015) emphasizes how blockchain technology through smart contracts can improve the efficiency of the banking system and reduce transaction costs. However, other studies have shown that while blockchain can improve the accuracy and speed of financial transactions, network scalability and defense against cyberattacks are major issues (Pilkington, 2016). In addition, constantly changing regulations make using this technology in the financial sector more difficult (Yermack, 2017).

However, previous research has not covered the regulatory and technical aspects of blockchain implementation in the banking industry. Studies on fintech and cyber security show that the industry is at a tipping point where new technologies must be utilised due to strict regulations and data security (ISACA, 2019; Tapscott & Tapscott, 2016). In addition, the

approach to privacy of blockchain-based systems is still a big issue. This is especially true for ensuring that transparency and protection of user data remain in balance (ISACA, 2020; Atzori, 2017).

Therefore, this study aims to fill the gap in the literature by further exploring the application of blockchain in the banking industry. The main focus of this research is to analyze the impact of blockchain on data security, regulation, and business efficiency within the banking sector, as well as provide strategic recommendations for companies looking to adopt this technology. The novelty of this article lies in its holistic approach that combines technical, regulatory, and business aspects in one analytical framework.

As such, this research is expected to increase stakeholders' understanding of how blockchain can be safely and effectively applied in the banking industry and help them make more informed and strategic technology-based decisions.

METHODS

This research uses the PRISMA method and the Systematic Literature Review (SLR) approach. PRISMA was used to compile a systematic and transparent literature review with the steps shown below:

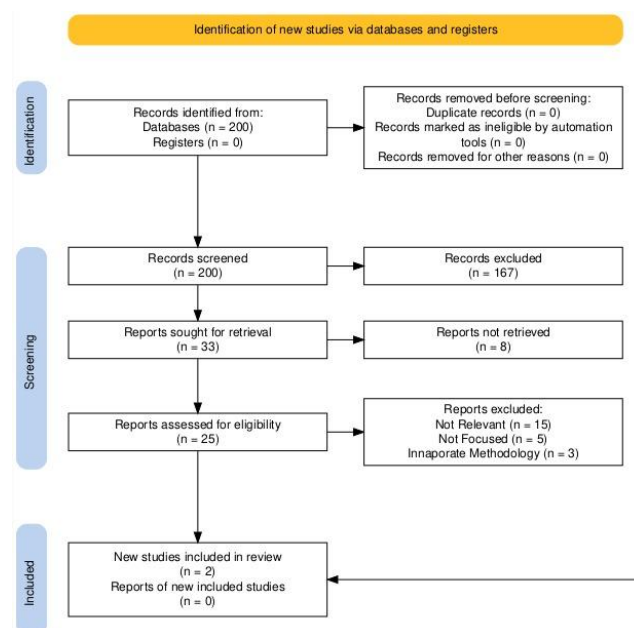


Chart 1 Method Framework with PRISMA

RESULT AND DISCUSSION

Data Analysis Using Publish Or Perish

Publish or Perish software helps researchers analyze and evaluate scientific publications that have been published. Below are the search

results using Publish or Perish with the keywords 'Data Security Management. Banking and Financial Services; COBIT 2019' for the last 10 years, starting from 2015 to 2025 and there are 200 journals that have application citations Through these journals, we then analyzed and visualized the relationships in the bibliometric data using VOSviewer software.

Data Analysis Using Vosviewer

VOSviewer is software used to analyze and visualize relationships in bibliometric data, such as keyword networks, collaboration between authors, and relationships between journals and institutions. The software was developed by the Center for Science and Technology Studies (CWTS) of Leiden University, the Netherlands. Through the VOSviewer software, we analyzed using normalization analysis with the strength of association method. The analysis showed three main colors, red, green, and blue, each representing a cluster, red for cluster 1, green for cluster 2, and blue for cluster 3. Each cluster has different item characteristics. Based on the analysis of 200 journals using VOSviewer software with the association strength method. the results are 11 items, 3 clusters, 46 links, and a total link strength of 1113.

Table 1 Cluster Based on VosViewer

Cluster	Item
<i>Cluster 1 (Red)</i>	1. Cobit 2. Governance 3. Information Security Management 4. Itil 5. Research
<i>Cluster 2 (Green)</i>	1. Bank 2. Framework 3. Impact 4. Risk
<i>Cluster 3 (Blue)</i>	1. Implementation 2. Security Management

Figure 1 is the result of Network Visualization using VOSviewer, in this study grouping key concepts into three clusters, namely red cluster, green cluster, and blue cluster, each of which illustrates an important aspect of data security management

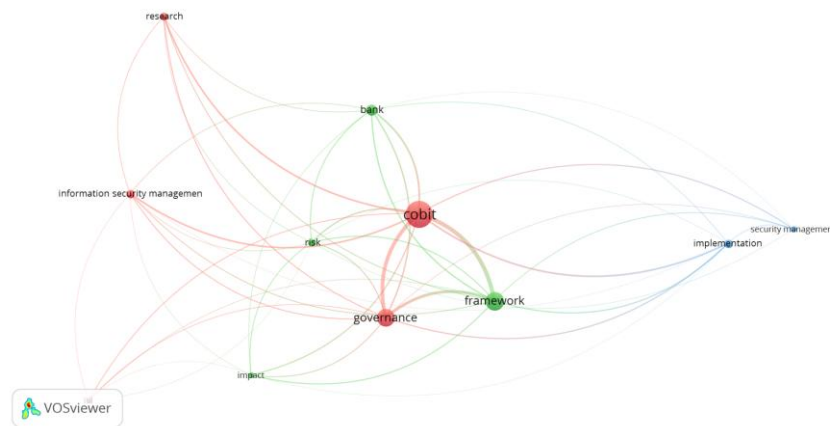


Figure 1 Network Visualization.

Overlay Visualization

Overlay Visualization in VOSviewer is one of the visualization methods used to display the trend or development of a topic based on bibliometric data. In this mode, each node (keyword, term, or reference) is assigned a color based on the timing of its appearance or impact in the research. Dark green indicates terms that appeared first in the research (around 2020-2021) including Risk, Governance, Framework, Implementation, Security Management, Impact. Light green to yellow colors indicate more recent and recently researched terms (around 2022) including Research, Information Security Management, Cobit, Bank.

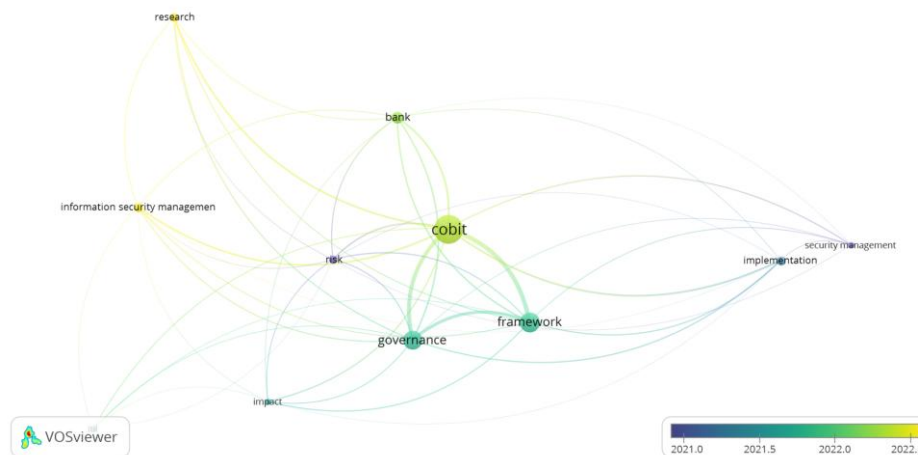


Figure 2 Overlay Visualization

Density Visualization

Density Visualization assists in analyzing the distribution of terms in a study, making it easier to identify key trends and provide insight into topics that have significant influence in a field of study. The analysis results show that a bright yellow color appears on the items Cobit, Framework, and

Governance, indicating that these three terms have a high degree of density and relatedness in the analyzed dataset. Fainter colors are seen in other terms, such as Bank, Risk, Research, Information Security Management, Impact, and Security Management Implementation, which indicate lower relatedness compared to the main items.

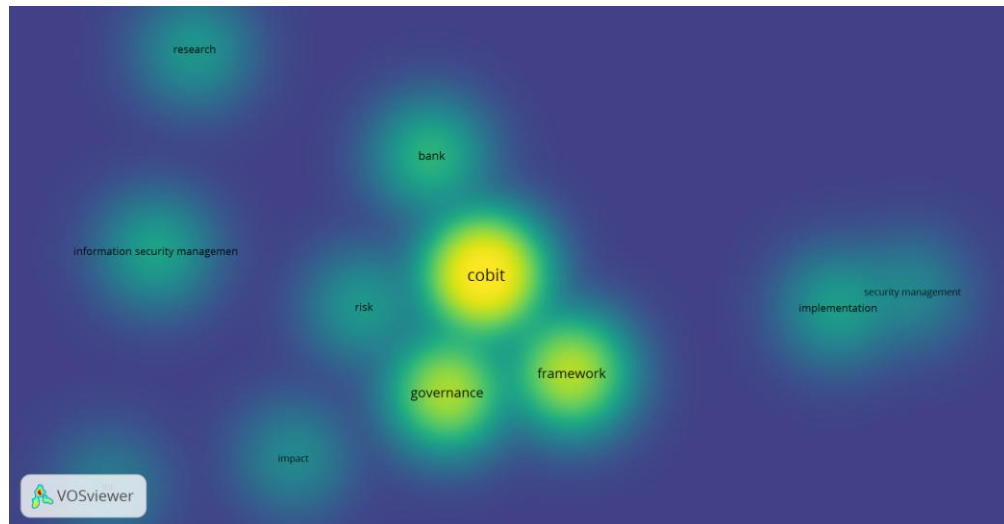


Figure 3 Density Visualization

The results of the Cluster Visualization analysis show the existence of three clusters with different colors, which represent the relationship between terms in the study. Cluster 1 (red) consists of Cobit, Governance, Information Security Management, Itil, Research, which indicates a close relationship between aspects of information technology governance and data security management. Cluster 2 (green) includes the terms Bank, Framework, Risk. Impact which indicates a focus on financial aspects, risks, and the application of the framework in the banking industry. Meanwhile, Cluster 3 (blue) consists of Implementation and Security Management which represents the implementation aspect of information security policies in a system.

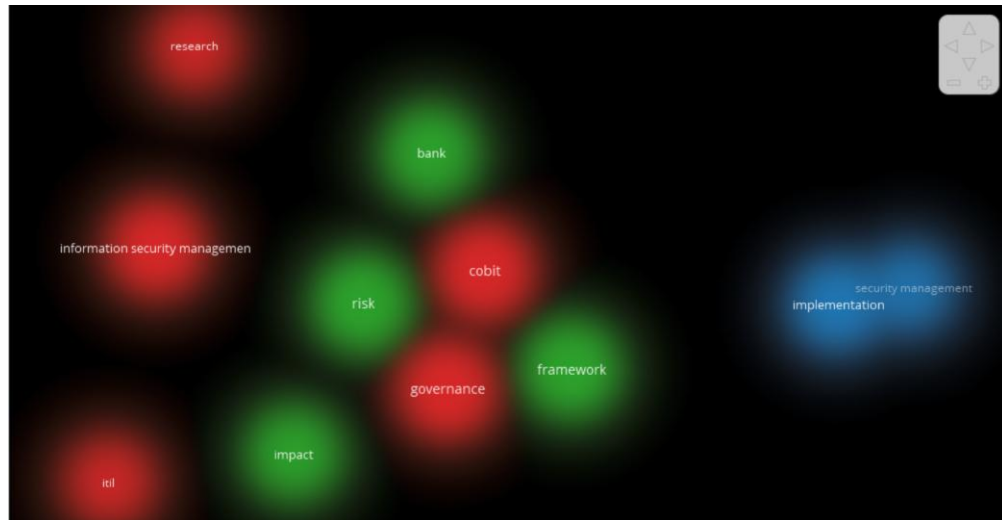


Figure 4 Cluster Visualization

Data Analysis Using Excel

Search results using Publish or Perish with the keywords "Data Security Management, Banking and Financial Services; COBIT 2019" for the last 10 years, namely 2015 to 2025, showed 200 journals that had citation and patent records. Then, from the 200 journal data, we identified 39 journal data that used PDF type by filtering the type by only selecting journals with that type. After identification, we found 39 journals that use PDF type.

The second stage is filtering. After obtaining 39 journal data using PDF type, we filtered the publishers by only selecting credible publishers. Thus, after the filtering process, we obtained 29 journal data published by credible institutions.

The third stage is feasibility, after obtaining 29 journal data published by credible institutions, we filter journal abstracts that are suitable and related to the banking we will analyze so that we get 9 journal data that are in accordance with the topic we will analyze, namely topics that are still related to the keywords "Data Security Management; Banking and Financial Services; COBIT 2019" in the Jast 10 years, namely 2015 to 2025. From the 9 journal data included, we analyzed the publisher's name. The results of our analysis show that there are 4 publisher names, namely mdpi, with a total of 10 citations or a large percentage of 42%, isac with a total of 13 citations or a large percentage of 54%, cyberleninka.ru with a total 1 citation or 4%. dspace.unza.zm with a percentage of 0%.

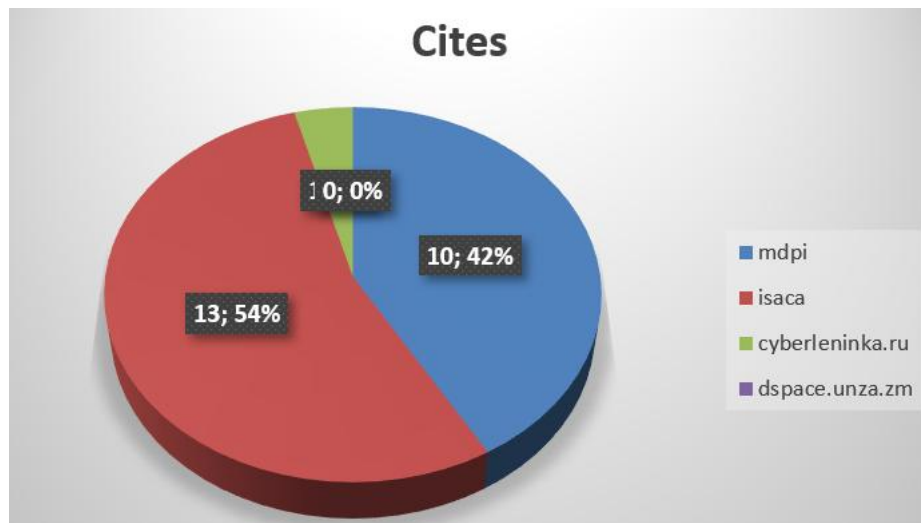


Diagram 1 Top Publishers Circle

Table 2. Top 29 Cited Authors in Research

No	Penulis	Sitasi
1	HM Melaku	33
2	P Solana-González, AA Vanti, MM García Lorenzo...	28
3	BD Tarbiyatuzzahrah, R Mulyana...	10
4	LN Kaliyaperumal	12
5	A Valackiene, R Andrijauskaite	10
6	G Pearce	15
7	JF Andry, S James, S Christian...	12
8	F Caron	16
9	SG Kassa, C Cisa	15
10	S De Haes, A Joshi, T Huygh...	15
11	FX Adrian, G Wang	3
12	J Marchão, L Reis, P Ventura	7
13	S Saeedinezhad, A Naghsh	8
14	S Smith, A Garcia	4
15	H Fasihuddin, S Alharbi, A Alshehri, A Alzahrani...	3
16	T Wang	9
17	S De Haes, A Joshi, T Huygh, S Jansen	8
18	I Markina, D Diachkov	5
19	C Vimal Mani	6
20	Y Razack, I CISA	2
21	G Roboff	6
22	BR Shubhamangala, S Saha	4
23	LE Alvarez-Dionisi	1
24	C Vimal Mani	1
25	RG JOIN, S JOIN, W ARE	2
26	LE Alvarez-Dionisi	1

27	TH Thabit, HS Ishhadat, OT Abdulrahman	1
28	C Vimal Mani	1
29	PD Bagus, W Lily	1

Cybersecurity as a Key Pillar in Digital Finance

In the digital age, cybersecurity threats are increasing, especially in the financial sector where valuable data and assets are stored. Cyberattacks, such as malware and identity theft, are becoming a serious challenge faced by banks and financial companies. Hence, it is critical for the monetary division to execute compelling security measures to secure their frameworks from cyber dangers. Great corporate administration will guarantee occasional evaluation of the organization's whole security system and its related exercises for each nation in which it works (Pearce, 2020).

One of the strategies used in cybersecurity is the utilization of artificial intelligence (AI) and machine learning to detect suspicious activity in financial transactions. This technology allows banks to identify anomalies and potential threats before theft or fraud occurs. Thus, security risks can be minimized, and financial transactions become more secure. Cyber threats such as malware hackers targeting the SWIFT system, set up by the Society for Around the world Interbred Money related Media transmission (Quick), are utilized by banks and monetary administrations organizations around the world to safely transmit data almost monetary exchanges. The level of advancement of the malware was illustrated by a later cyberattack on the Quick infrastructure/self-service cash machine (ATM) of India's moment biggest bank (Mani, 2019).

Many banks are starting to adopt hybrid identity solutions, which are authentication systems that combine various identity verification methods. With this system, only truly authorized individuals can access data or perform financial transactions. This makes hacking attempts more difficult for irresponsible parties.

According to Mani (2019), explaining how to overcome cybersecurity risks, are as follows:

- Maintain a strategic distance from utilizing open clouds that are inclined to the chance of information spillage
- Revive bequest IT foundation and center keeping money frameworks.
- Utilize machine learning successfully to make strides the cybersecurity pose of fintech businesses.
- Execute a computerized personality assurance arrangement.
- Institutionalize well-defined third-party security measures.
- Inquire about acquirement arrangements innovation innovation arrangements from a security point of see.

- Reinforce get to control instruments.
- Actualize well-defined information protection rules.
- Consider executing security coordination arrangements Security Coordination and Robotized Reaction (Take off), Security Operations and Analytics Stage Engineering (SOAPA), and Client and Substance Behavior Investigation (UEBA), which help in proactive occurrence reaction.
- See overhauled risk insights through danger nourishes and robotized endpoint location (EDR)/managed discovery and reaction (MDR) arrangements

However, the biggest challenge in cybersecurity comes from the human factor. Many users still use weak passwords or are easily fooled by phishing attacks through fake emails. Therefore, banks need to increase education and training for their customers and employees to be more aware of cyber threats. By raising awareness of the importance of digital security, the financial sector can be better protected from the threat of data theft and fraud.

Digital Transformation in Banking and Financial Services

The development of technology has changed the way modern banking works. Today, banks not only rely on conventional services, but also utilize advanced technology to improve efficiency and convenience for customers. Some of the main innovations in banking digital transformation include the use of AI-based chatbots for customer service, data analysis to understand customer needs, and transaction automation to increase service speed. According to Dionisi (2021) A more productive way to overcome this circumstance is to associated with managing an account bots, when utilizing managing an account bots, clients can straightforwardly chat with bots and rapidly get answers to their questions.

However, the process of digital transformation in the banking sector is not free from various challenges. According to Dionisi (2021) examples of bot risks include:

- Wrong reactions, In case bots are deficient rules or scripts, they might grant wrong reactions to clients.
- Defenselessness, When bots are helpless, aggressors can take advantage of the bot's shortcomings, which can lead to the misfortune of delicate information and data. Such scenarios incorporate hacking, phishing, and other cyberattacks.
- Need of encounter, This happens when the conclusion client has restricted or no involvement utilizing the bot. As a result, this

circumstance avoids the conclusion client from having a smooth exchange with the bot.

- Need of administrative compliance required, In this case, government money related controllers manage bot client interaction Rules to ensure shoppers from obfuscatory behavior and ensure straightforwardness of operations. Subsequently bots are required to comply with government commands inserted in inner rules or scripts. On the off chance that the bot does not comply with government directions, the organization might deceive the user's alternatives, subliminally coerce the user's activities and exhort the client to select pointless items and administrations.
- Debasement of organize execution, Human-bot-human sessions can completely utilize organize Transfer speed. In this manner, a nitty gritty examination of arrange Capacity and measure ought to be considered some time recently bot usage.
- Need of administration structures and methods, Need of structures and methods can result in moo operational effectiveness, which can lead to venture misfortunes.

Customer data management is a crucial aspect of digital transformation. The more data a bank collects, the greater the security risks. Information spillage can have a critical negative affect on both clients and the bank's reputation. Information misfortune may be a common and perpetual issue confronted by worldwide organizations that has no single silver bullet arrangement. Organizations ought to consider leveraging various best hones around DLP actualizing the leading DLP arrangement that will way better suit wants of the organization (Mani, 2019). Therefore, digital transformation strategies must be accompanied by strict data protection policies and compliance with applicable regulations.

By implementing the right measures, banks can continue to thrive in an increasingly competitive digital ecosystem. Banks can offer services that are more efficient, secure, and in line with contemporary customer needs if digital transformation goes well. As such, digital banking can continue to evolve as a key pillar in the future financial industry.

IT Governance in Digital Banking and Finance

Modern banking relies heavily on information technology (IT) to manage various financial transactions and customer data. Therefore, an effective IT governance system is required to keep all banking operations running IT governance provides a structure that links processes, IT assets, and data to the company's technique and corporate goals. In expansion, IT administration coordinating and institutionalizes ideal ways of arranging and organizing, securing and executing, conveying and supporting, observing IT execution (Prasetyo, 2019). So IT governance covers various aspects,

including risk management, regulatory compliance, and optimization of available technology resources.

COBIT (Control Objectives for Information and Related Technologies) is a framework used in banking IT management. COBIT, may be a general standard for IT administration, with the most objective of characterizing the organizational forms required for IT to meet trade goals, this standard separates IT operations into 34 forms, extending from methodology to advancement, operations and bolster (Prasetyo, 2019). COBIT provides guidelines for banks in managing IT assets, identifying risks, and ensuring that the technology systems used can operate safely and efficiently. According to Tarbiyatuzzahrah (2023) If the IT strategy is aligned with the organization's business strategy, strategic alignment will be better, which means the organization's performance will be better too. By implementing good IT governance, banks can ensure that customer data is protected, operational systems are always in optimal condition, and technological innovations can be implemented without posing significant legal risks. According to Tarbiyatuzzahrah (2023):

- Plan Plan and Organize (PO)
Discuss strategies and tactics and how best to help achieve business goals.
- Acquire and Implement (AI)
Responsible for realizing the information technology strategy. which means that information technology must be identified, developed, or discussed, and implemented integrated in business processes.
- Deliver and Support (DS)
Relates to the delivery and support of information technology to people who need support to do their jobs.ini.
- Monitor and Evaluate (ME)
All IT processes must be evaluated regularly to ensure their quality and to ensure that they comply with control requirements. Work management, regulatory compliance, internal control monitoring, data management are all topics covered in this area.

A key challenge in banking IT governance is finding a balance between innovation and regulation. Technologies such as artificial intelligence, cloud computing and blockchain provide many benefits to the banking sector. However, without clear regulations, the application of these technologies can pose various risks, such as data leakage, cyber attacks, and non-compliance with applicable regulations. Therefore, banks should implement policies that allow flexibility in technological innovation, while ensuring that security and compliance aspects are maintained.

Banks also need to regularly review and update their IT strategies to stay aligned with the latest technological developments. Research results by Tarbiyatuzzahrah (2023) explain that IT resources must be able to check the security controls in use, including updates, and oversee access rights to view, mod and submit data delete requests. This includes investing in cybersecurity systems, improving customer data protection, and implementing technology solutions that suit business needs. With the right IT strategy, banks can continue to thrive in an increasingly complex and competitive digital ecosystem.

The Role of Blockchain Technology in Digital Finance Security and Governance

Blockchain is a technology that functions as a distributed and immutable digital ledger. Mani (2017) states that Blockchain is a distributed database, which protects a growing list of records from and is safe from tampering and revision. Meanwhile, according to Dionisi (2021) blockchain is a shared ledger of transactions across a network of multiple nodes without relying on a single trusted central authority. Every transaction recorded in the blockchain is permanent, making it one of the secure and transparent technologies in the financial world. The main advantage of blockchain is its ability to eliminate intermediaries in financial transactions, such as banks or other financial institutions.

According to Mani (2017), based on thousands of hubs in a peer-to-peer blockchain arrange, exchange information is duplicated and overhauled at each hub, indeed in case one of the hubs clears out the arrange inadvertently, intentioned or gets to be blocked off, the organize as a entirety will proceed to work, this guarantees that the blockchain framework is profoundly accessible and blockchain innovation guarantees an awfully tall level of security of exchanges enlisted into the blockchain through the cryptographic innovation utilized in building the blockchain. Thus, transactions can be made more securely.

In addition, blockchain also has various applications in the financial world, such as cross-border payments, smart contracts, and digital identity protection. Smart contracts, when combined with data analytics and continuous auditing and monitoring, can revoke transactions that do not comply with company policies or detect processes that violate internal business rules, and smart controls can self-adjust to support, flexible, and timely assurance (Smith, 2022).

This technology allows financial transactions to be more transparent and reduces the possibility of fraud. However, despite its various advantages, blockchain still faces security challenges, especially from the threat of hacking. As for the challenges of blockchain as explained by Smith (2022) due to the need of a centralized specialist to confirm the presence,

propriatorship, or estimation of exchanges recorded on the blockchain, permissionless blockchains may show the foremost difficult challenge in that there's no centralized specialist to report cyberattacks, extortion, or other security dangers. Therefore, efforts to improve security in blockchain technology are ongoing to strengthen the protection of these systems. Different countries have different approaches to blockchain. Some countries have adopted regulations that support the development of this technology, while others are still in the exploratory stage or even show skepticism. To encourage the widespread adoption of blockchain, a balance between regulation and innovation is needed so that this technology can develop optimally without hindering the progress of the financial industry.

The development of blockchain technology continues. This is expected to increase efficiency and flexibility in the use of blockchain in various sectors. With the continued development of this technology and solutions to existing challenges, blockchain is projected to have a bright future in the global financial industry.

Case Study: COBIT 2019 Implementation at XYZ Bank

Bank XYZ is a concrete example of a banking institution that has successfully implemented COBIT 2019 in managing their IT infrastructure. By adopting this framework, Bank XYZ is trying to improve information technology governance to be more structured and in accordance with existing regulations. In many fintech companies in Indonesia have also started implementing COBIT 2019 to strengthen risk management and IT governance. The implementation of COBIT 2019 in the fintech industry helps these companies to stay relevant and competitive amidst the rapid changes in the financial sector.

With a value- and outcome-based approach, financial organizations can more easily formulate strategies that align with business objectives and mitigate risks arising from the use of information technology. COBIT 2019 provides principles and best practices that make it easier to develop strategic plans while efficiently managing operational activities. The success achieved by Bank XYZ can be a valuable reference for other financial institutions in making COBIT 2019 the foundation of their IT management, in order to achieve optimal performance.

The implementation of COBIT 2019 at Bank XYZ provides impressive evaluation results and lessons for organizations in the financial industry. The results show that objective domains APO12 (Managed Risk), DSS03 (Managed Problems), and DSS04 (Managed Continuity) have a level 3 capability value. In contrast, objective domains DSS02 (Managed

Service Request and Incidents) and DSS05 have a level 2 capability value. The results show how XYZ bank currently manages its IT network infrastructure (Hermawan et al., 2022).

The results of research conducted at Bank XYZ show that there are two levels capability which berbeda in network infrastructure management, based on an evaluation using the COBIT 2019 framework. In the APO12 (Managed Risks) and DSS03 (Managed Problems) domains, Bank XYZ reached level 3 (Established), which means that the processes implemented more organized and well defined. According to research, this process is usually referred to as "good" and is defined as "the process of achieving goals in a more organized way using organizational strategies" (Hermawan et al., 2022). This indicates that the department has an established system for identifying and managing risks and resolving problems, which is a positive indicator for managerial success.

However, for domains DSS02 (Managed Service Requests and Incidents) and DSS05 (Managed Security Services), the evaluation resulted in level 2 (Managed). This means that while there is some structure in place, there are still many weaknesses in the implementation of a more comprehensive process. "This process achieves objectives through the application of a basic, complete, and set of activities that can be characterized as performance" (Hermawan et al., 2022). This suggests that despite progress, further investment in process development is necessary to drive overall performance and avoid risks that could arise from deficiencies in incident management and security.

Overall, as a result of the evaluation, XYZ Bank is on track in their IT management. However, with the gaps found between the achieved and expected levels, there is an urgent challenge to improve capability in areas that are still at a lower level.

From the results of this research, there are several valuable lessons that can be learned for further development in IT management at Bank XYZ. First, the importance of applying the COBIT 2019 framework as an evaluation and improvement tool in IT infrastructure management. By using a systematic approach, Bank XYZ has been able to get a clear picture of their current performance and areas that require improvement. As explained, this research was conducted to evaluate the service management capacity of IT network infrastructure based on COBIT 2019 (Hermawan et al., 2022). This underscores the significance of using a recognized standard to identify weak points and strengths.

Second, another lesson learned is the need for better risk management. Although XYZ Bank received a positive assessment in risk management, this does not exclude that many aspects still need strengthening. This is driven by the fact that according to Hermawan et al.

(2022), the Infra Division has important information about IT network-specific events, but it has not been used regularly. This shows that proactive management and routine in monitoring and evaluating risks are essential to achieve higher levels.

Finally, the importance of communication and collaboration between teams is also one of the most important factors. Processes that must be carried out in depth require contributions from various departments, and the active involvement of all members of the organization in achieving goals is expected to increase the overall effectiveness of IT management. This research clearly shows that success in management. This research clearly shows that success in IT infrastructure management depends not only on the procedures implemented but also on the way teams collaborate in carrying out their tasks.

CONCLUSION

This research provides a comprehensive overview of the importance of data security in the banking industry in the digital era, where cyber threats and regulatory demands are increasing. Through a Systematic Literature Review (SLR) approach with the PRISMA method, as well as bibliometric analysis using Publish or Perish and VOSviewer to identify research trends from 2015 to 2025, this study identifies research trends in data security management. In addition, blockchain technology is proven to increase transparency and security of financial transactions by reducing the role of intermediaries, although it still faces challenges in terms of scalability and regulation. The implementation of COBIT 2019 at XYZ Bank shows that the use of this framework has helped improve IT governance in a more structured and regulatory compliant manner. The capability evaluation shows that Bank XYZ has reached level 3 (Established) in risk management (APO12) and problem management (DSS03), signifying more organized and well-defined processes. However, in service request and incident management (DSS02) and security services (DSS05), the bank is still at level 2 (Managed). indicating weaknesses and the need for further strengthening.

In the digital financial ecosystem, cybersecurity is a key pillar that determines the sustainability of the banking system. The use of artificial intelligence (AI) and machine learning has helped detect anomalies in transactions and improve protection against cyber-attacks, such as those on SWIFT infrastructure. However, challenges such as implementation complexity, high costs, and the dynamics of regulatory changes are still obstacles in optimizing security systems. Therefore, this study recommends

a risk-based approach to IT governance, increased cybersecurity awareness in the work environment, and the integration of cutting-edge technologies such as blockchain and AI to strengthen data protection systems. With more adaptive regulatory policies and innovative governance approaches, the banking industry can optimally utilize digital technology without compromising security and compliance aspects.

Advice

Based on the research results, there are several steps that can taken by the banking industry to strengthen their data security systems. First, banks are advised to implement a risk-based security strategy tailored to their specific needs, utilizing COBIT 2019 as the main guide. Second, cyber awareness among employees and customers needs to be strengthened through regular training and educational campaigns, especially to recognize threats such as phishing and ransomware. Third, the use of cutting-edge technologies such as artificial intelligence (AI) and multi-factor authentication (MFA) can improve threat detection and data protection.

Addition, banks should also consider the adoption of blockchain technology carefully, ensuring there are supportive regulations and solutions to address scalability challenges. Collaboration with regulators, other financial institutions, and third-party vendors is also essential to create a more resilient security ecosystem. Finally, banks need to regularly evaluate and update their IT strategies to stay relevant to the latest technological and regulatory developments, so they can continue to compete in an increasingly complex digital world.

Research Limitations

This study has several limitations that need to be noted. First, the SLR approach with the PRISMA method and bibliometric analysis is limited to data from Publish or Perish and VOSviewer, which may not cover all relevant literature from other sources, such as specific academic databases. Second, the lack of primary data from customers or external parties makes it difficult to understand the direct impact of data security on public trust. Third, the discussion on blockchain is more theoretical and has not been supported by in-depth empirical studies, so the analysis is still limited to the existing literature.

Further Research

To develop further understanding, future research is recommended to expand the scope of case studies to more banking institutions or even

the fintech sector, so as to provide a broader picture of the effectiveness of COBIT 2019 and blockchain. Research could also combine qualitative approaches, such as interviews with customers and bank employees, as well as quantitative through surveys, to gain a more comprehensive perspective on data security. In addition, an in-depth exploration of the integration of blockchain with other IT governance frameworks, such as the NIST Cybersecurity Framework or ISO/IEC 27001, could provide additional insights into more optimized security solutions. Finally, research could focus on the direct impact of this technology on customer trust and bank financial performance, involving empirical data from the field.

REFERENCES

- Hermawan, S. D., Hermadi, I., & Nurhadryani, Y. (2022). Evaluasi capability level infrastruktur jaringan ti bank xyz menggunakan cobit 2019. *Syntax Lit. J.*
- Valackiene, A., & Andrijauskaite, R. (2021). Model for assessing information logistics systems in banks: Lithuanian case study. *Logistics*, 5(3), 42.
- Vimal Mani, C. I. S. A. (2017). A view of blockchain technology from the information security radar. *ISACA J.*, 4.
- Smith, S., & Garcia, A. (2022). Blockchain Smart Contracts, Part 1: Introduction for Accounting and Auditing Professionals. *ISACA Journal*, 4, 1-6.
- Alvarez-Dionisi, L. E. (2021). To bot or not to bot? That is the question for digital banking. *ISACA Journal*, 4, 26-30.
- Alvarez-Dionisi, L. E. (2021). Technology-based trust with blockchain. *ISACA Journal Online*, 1-4.
- Vimal Mani, C. I. S. A. (2019). Cybersecurity and Fintech at a Crossroads.
- Mwanza, L. P. (2020). *Information and communication technology security governance in Zambian banks* (Doctoral dissertation, The University of Zambia).
- Bagus, P. D., & Lily, W. (2019). Audit the implementation of information technology governance in financial services company using cobit 4. 1 framework. *International Journal of Open Information Technologies*, 7(11), 86-93.
- Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, 3(3), 327-350.
- Solana-González, P., Vanti, A. A., García Lorenzo, M. M., & Bello Pérez, R. E. (2021). Data mining to assess organizational transparency across technology processes: An approach from it governance and knowledge management. *Sustainability*, 13(18), 10130.

- Tarbiyatuzzahrah, B. D., Mulyana, R., & Santoso, A. F. (2023). Penggunaan COBIT 2019 GMO dalam menyusun pengelolaan layanan TI prioritas pada transformasi digital BankCo. *JTIM: Jurnal Teknologi Informasi dan Multimedia*, 5(3), 218-238.
- Kaliyaperumal, L. N. (2021). The evolution of security operations and strategies for building an effective SOC. *ISACA Journal*, 5, 1-7.
- Andry, J. F., James, S., Christian, S., & Dela, H. (2019). Evaluation and recommendation it governance in hospital base on cobit Framework. *International Journal of Open Information Technologies*, 7(5), 51-58.
- Caron, F. (2017). Blockchain: Identifying risk on the road to distributed ledgers. *ISACA Journal*, 5, 1-6.
- Kassa, S. G., & Cisa, C. (2017). IT asset valuation, risk assessment and control implementation model. *ISACA J*, 3(1), 1-9.
- De Haes, S., Joshi, A., Huygh, T., & Jansen, S. (2017). Exploring how corporate governance codes address IT governance. *ISACA Journal*, 4, 1-7.
- Adrian, F. X., & Wang, G. U. N. A. W. A. N. (2023). Measure the Level Capability IT Governance in Effectiveness Internal Control for Cybersecurity Using the COBIT 2019 in Organization: Banking Company. *Journal of Theoretical and Applied Information Technology*, 15(5).
- Marchão, J., Reis, L., & Ventura, P. (2020, October). Operation management using ITIL and COBIT framework. In *Conference Proceedings (part of ITEMA conference collection)* (pp. 201-207).
- Saeedinezhad, S., & Naghsh, A. (2019). Management of IT Services in the Field of Pre-Hospital Emergency Management with the Combined Approach of COBIT Maturity Model and ITIL Framework: A Conceptual Model. *Health Management & Information Science*, 6(3), 85-95.