International Journal of Information System & Technology
Akreditasi No. 158/E/KPT/2021 | Vol. 6, No. 6, (2023), pp. 785-792

An Narative Review on Achieving Data Governance in Indonesia Amidst Data Security Challenges

Widia Febriyani[1], Tien Fabrianti Kusumasari[2], Muharman Lubis[3]
[1,2,3]Telkom University, Bandung, Indonesia
Email: widiafey@student.telkomuniversity.ac.id[1],*
tienkusumasari@telkomuniversity.ac.id[2], muharmanlubis@telkomuniversity.ac.id[3]

Abstract

This article discusses strategies to achieve good data governance in Indonesia amidst data security challenges, including data security cases that have occurred in Indonesia. According to the IT Governance Institute (ITGI) in 2021, only 34% of companies in Indonesia have implemented good data governance standards. This indicates a gap in understanding between organizations, as they have not fully realized and understood the importance of data governance. This study used a narrative review as a methodology to evaluate relevant studies related to this topic. The findings show the importance of sustainable data governance and cybersecurity, but only a small portion of organizations in Indonesia have implemented data governance strategies or data intelligence solutions. This article highlights strategies to improve data security in data governance in Indonesia through a better understanding of information security practices. The Data Management Association (DAMA) International Guide to the Data Management Body of Knowledge (DMBOK) concept is used as a conceptual framework for this research. This article provides significant information on strategies to improve security practices in data governance and the safe use of data, which can improve economic well-being.

Keywords: *DAMA, Data Security, Strategy, Data Governance, Indonesia*

1. Introduction

In the current era of digitalization, information security has become an increasingly important issue for organizations. Data breaches, system shutdown attacks, and malicious software can harm organizations and threaten business continuity. Therefore, it is important for organizations to have a sustainable data governance strategy and to pay attention to the security aspects of corporate information in order to maintain the quality of organizational data [1]. The quality of organizational data can be seen from three aspects: confidentiality, integrity, and availability of data. Confidentiality of data means that authorized individuals can only access data, while data integrity means that the data is not tampered with or altered without the knowledge of the data owner. Meanwhile, data availability means that data can be accessed securely and stably anytime and anywhere [2]. To maintain the quality of organizational data, a company's data governance strategy needs to be adopted along with corporate information security. However, it is not enough to only have a strong data governance and information security strategy, but it is also important to teach employees how to behave safely and responsibly with the data held by the organization [2]–[4].

In the field of information system security, the use of organizational data decision-making rights, rules, protocols, and policies is crucial to prevent, detect, and respond to security incidents that may challenge to implement data security on data governance. Data security for effective information system security management of organizational data depends on the improvement of protective technology and policy compliance among data networks and employees [5], [6]. However, the existing information system security management model overly emphasizes the rationality of decision makers [7], and the decision-making rights, rules, and protocols for data and related data processes [3], [8]. Therefore, there needs to be a broader and more holistic understanding in managing

ISSN : 2580-7250

information system security, involving the entire organizational structure rather than just a small part of it. This will help organizations to respond quickly and effectively to security incidents, and improve employee awareness and compliance in managing data safely and responsibly [9].

The issue of data security in Indonesia is becoming increasingly important given the rapid growth in the use of information technology and the internet in the country. There have been several cases of data security breaches in Indonesia in recent years. One of these cases involved a data breach at the e-commerce site Tokopedia in 2019, where approximately 91 million user data were exposed, including full names, email addresses, phone numbers, and other information. This case demonstrated that even large e-commerce websites are vulnerable to cyber-attacks. Another data breach occurred at the e-commerce site Bukalapak in 2020, where around 13 million user data were exposed, including full names, email addresses, and other information [10]–[12]. In 2020, there was a data leak at BRI Agro, a subsidiary of PT Bank Rakyat Indonesia (Persero) Tbk. It was reported that around 2 million customer data was leaked, including names, addresses, birth dates, phone numbers, and other information. This incident shows that data security in the banking sector in Indonesia still needs to be improved [13].

In 2020, there was also a case of online fraud in Indonesia, where scammers tricked victims by sending links to fake websites and stealing their personal information, including phone numbers, email addresses, and credit card information. Statistics on data security in Indonesia are still limited, but according to a report by Kaspersky in 2020, Indonesia ranked fourth in the world for the number of cyber-attacks. These attacks include malware, phishing, and DDoS attacks [14]. The report also mentioned that most cyber-attacks in Indonesia occur in the banking and e-commerce sectors. Therefore, data security is becoming increasingly important for companies in Indonesia to protect their businesses and customer data [14], [15].

To secure data, there are several actions that can be taken. One of them is using a strong password consisting of a combination of letters, numbers, and special characters. In addition, make sure the system and applications are always updated and install the latest security patches [16]. To protect the system from malware and viruses, antivirus software and firewalls should always be installed [17]. Use two-factor authentication on your account for added security. Always be cautious when giving out personal information and regularly back up your data to an external hard drive or cloud storage. Finally, security training needs to be provided so that users understand the importance of properly protecting data. By taking these actions, data can be protected from security risks and potential problems can be avoided [18].

The importance of data security cannot be overstated in today's digital age, where information is constantly being shared, stored, and transmitted across networks. However, ensuring the security of data is not an easy task and presents various challenges that need to be addressed [18]. Therefore, this study aims to conduct a comprehensive literature review and comparative analysis of the challenges and implementation points of data security. The study will explore various sources such as academic journals, books, and online resources to gain insights into the current state of data security, including the latest trends, technologies, and best practices [3], [18]. Furthermore, the study will compare different approaches and solutions for data security, including encryption, firewalls, access controls, and intrusion detection systems. By conducting this research, it is hoped that the findings will contribute to the development of effective data security strategies and help organizations to better protect their sensitive information from potential threats and risks.

2. Literature Review

2.1. Data Governance

The concept of data governance is very important in data management within an organization as it relates to efforts to ensure the accuracy, security, and availability of data that is collected, stored, and used within the organization. The absence of data governance can lead to risks such as data loss, data leakage, and other problems [19]–[21]. Therefore, every organization must have clear policies and procedures in data management to ensure the security and integrity of data. Data governance responsibility is not just on one department or individual, but jointly by all members of the organization [4]. Everyone must understand the importance of maintaining data and protecting it from security threats and misuse [16], [22]–[24]. It is important for every individual in the organization to understand data governance policies, including how to collect data, manage and store data, and how to use data to support the organization's goals. In the increasingly connected business era, data governance has become increasingly important. Data generated by an organization can be used for smart and strategic business decision-making, but it can also be a dangerous weapon for the organization if used improperly. Therefore, paying attention to data governance is a key factor for success in the business world today [25].

The framework for data governance encompasses the creation of knowledge and strategies for managing data operations, preservation, curation, availability, quality, and also considers legal and policy aspects related to data management and security [26], [27]. Data governance is a decision-making process that focuses on establishing an authoritative structure to determine decision rights and responsibilities related to data use, security, integrity, and completeness. As the use of big data technologies for public policy and services continues to grow, organizations must create data policies and governance frameworks [20]. The use of digital technologies based on large volumes of data can give rise to significant issues, necessitating the development of tools to mitigate risks and define patterns of action for data stewards and analysts. When working with big data, data governance is necessary to ensure ease of use, security, and compliance with norms, guidelines, and rules. Information systems security failures can have serious consequences for sustainable development goals, including commercial liability, loss of credibility, and financial losses [21], [25], [28].

2.2. Data Security

Data security is a crucial concept in maintaining the safety and confidentiality of data within an organization. It relates to the efforts made to prevent unauthorized access, use, modification, theft, or loss of data. Without data security, organizations face the risk of data loss or breaches that can result in financial losses and damage to their reputation. Every organization should have clear policies and procedures in place to ensure data security and confidentiality [16], [18]. Data security is not the responsibility of just one department or individual, but rather a joint responsibility of all members of the organization. Every individual in the organization should understand the data security policies and be responsible for maintaining the security and confidentiality of data [23], [24]. In today's digital era, data security is even more important due to the increasing types of data collected and stored by organizations. Unprotected data can be easily misused or accessed by unauthorized parties, making data security a key factor for success in the business world today [29], [30]. Therefore, organizations must continue to improve their efforts in managing and protecting their data effectively.

Data privacy, also known as personal privacy, refers to an individual's right to maintain confidentiality and control over their personal information [31]. This concept is related to policies and practices in the collection, use, and dissemination of personal information. In today's digital age, data privacy has become increasingly important due to the growing

amount of personal information collected, stored, and shared through information technology [31]–[33].

2.3. Data Management Body of Knowledge

DMBOK (Data Management Body of Knowledge) is a comprehensive framework that provides a set of best practices and guidelines for managing data effectively. It covers ten areas of knowledge, including data and architecture management, data quality management, metadata management, master data management, data security management, data integration and interoperability management, data environment management, data project management, operational data management, and data governance and policy management [34]–[36]. The DMBOK framework helps organizations to standardize their data management practices, improve data quality, and ensure the security and confidentiality of sensitive data [37]. DMBOK is widely recognized as a standard reference for data management professionals and organizations, providing a common language and a shared understanding of key concepts and practices. The framework is regularly updated to reflect the evolving needs and challenges of the data management field [38], [39]. By following the guidance and best practices outlined in DMBOK, organizations can establish a solid foundation for effective data management, leading to improved data quality, better decision-making, and increased competitiveness. The framework also emphasizes the importance of collaboration and communication across different departments and stakeholders, helping to ensure that data is managed in a holistic and strategic way [40], [41].

3. Research Methodology

In this study, a narrative review approach was used, which is an accepted research methodology for comprehensive studies aimed at synthesizing a framework of research, identifying gaps and research opportunities, and providing a foundation for drawing holistic interpretations or conclusions based on existing theories, conceptual frameworks, and models within the scope of the review. The narrative review approach involves reviewing, analyzing, and integrating different approaches and research findings to exercise a holistic-content reading and draw conclusions based on the reviewers' experience, existing theories, and models. A narrative study approach is most suitable for a descriptive or explanatory study that allows for a narrative-constructivist and integration approach, mainly using narrative methods of data collection and analysis, and producing a final narrative report. Narrative review methodology has significant strengths, such as establishing platforms for comprehending diverse and numerous understandings derived from multiple data sources and research findings and acknowledging researchers' views and knowledge. To maximize the reliability and validity of data and interpretations, methodological triangulation was also used, which is a platform for engaging multiple sources of data to gain multiple perspectives and build a coherent justification of data interpretation.

The narrative review methodology has significant strength in creating a platform that can develop diverse understandings from various data sources and research findings. Furthermore, it provides an opportunity for researchers to engage in reflective practices and acknowledge their views and knowledge. Methodological triangulation, as a platform, involves multiple data sources to obtain diverse perspectives and maximize the reliability and validity of data, thus building a coherent justification of data interpretation. Methodological triangulation also helps to confirm the reliability and validity of collected information and provides a justification for the interpretation of the review."

In this study, our narrative review is focused on the aspects of data governance and information security within the context of cybersecurity. We recognize the importance of data governance as the foundation of cybersecurity, which ensures that organizational data is only accessed by authorized personnel and keeps company data secure. Our review

is limited to cybersecurity, which essentially involves confidentiality, integrity, and availability of organizational data protected by data governance programs to ensure secure data management across the organization. However, the data governance model only emphasizes data quality, and its scope is limited to this aspect.

4. Results and Discussion

Here are some statistics related to data governance management in Indonesia according to a survey by the IT Governance Institute (ITGI) in 2021, only 34% of companies in Indonesia implemented good data governance standards. In 2020, around 53% of companies in Indonesia experienced data breaches, according to a report by the cybersecurity research institute, Cybersecurity Indonesia. In a survey by Ernst & Young in 2021, 57% of respondents stated that their companies did not have clear data governance policies or procedures. Based on a report by the Indonesian Ministry of Communication and Information Technology in 2021, more than 90% of micro, small, and medium-sized enterprises (MSMEs) in Indonesia have not implemented good data governance standards. The statistics indicate that there are still shortcomings in data governance management in Indonesia, especially in small and medium-sized companies.

The implementation of data governance is not exempt from full support from stakeholders, including how information technology is utilized by the organization to produce optimal outputs that can be used in business processes or support the performance of the company or organization. Each stage needs to be monitored and regularly monitored to ensure that the main activities related to data, from input, process, technique to output, have complied with applicable standards and procedures. This compliance certainly needs to be supported by compliance with current standards.

Moreover, Indonesia has implemented Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which regulates individuals, including those engaged in business or e-commerce at home, can be categorized as personal data controllers. To achieve the goals of the company, the support of each stakeholder is needed to conduct identification of the best and centralized strategies to ensure that these goals are achieved. Each goal needs to be prioritized by considering the mapping of each initiative made by each unit. As for the requirements that must be met in making a strategy to be applied to the company, there are several important things to consider. First, there are general requirements related to the company's main business processes.

This is important considering that business processes need to be clearly and specifically defined. Second, there is the mapping of business processes into strategic goals of information technology and organizational goals, usually in the form of initiative programs identified by the organization. In addition, the third point is the management of the data governance model that will be identified, as well as the objectives of the implementation, whether it is to improve effectiveness and efficiency or to take initiatives to be implemented by the organization. Another important point is the roadmap of what will be done in one, two, or five years in the future as a future view of milestones to be achieved. The last point is the support of all parties in implementing data governance.

To improve data security in data governance, there are several strategies that can be applied. First, identify and classify data based on value, sensitivity, and importance. By doing this, more important and sensitive data will get a higher level of security. Next, create clear and detailed data security policies to ensure that the entire organization understands and consistently applies the policies. Providing training and awareness to users about data security policies and best practices in data management is also an important strategy to improve data security. Monitoring and auditing of data security systems regularly is necessary to ensure data security is maintained and potential security threats are detected. Identifying and evaluating data security risks and developing appropriate mitigation plans to reduce those risks should also be done. Additionally, installing data security solutions such as data encryption, access management, and

firewalls to protect data from security threats is an important strategy. Finally, periodically evaluating the implemented data security governance system and making necessary improvements and enhancements to continue protecting data from security threats.

5. Conclusion

Information security experts must strive to become proficient organizational security staff for their data by knowing the location of all organizational data, dividing it into distinct parts, and ensuring effective security measures between them. This division is necessary to contain the risk if a breach occurs in one section. Deleting low-value data and enforcing strict compliance regulations regarding data retention reduces the risk and minimizes the amount of data that can be infiltrated. Critical personal, financial, and health information should be stored in a controlled warehouse and all critical value data must be kept secure. Regular screening of email, file sharing, and unprotected systems is essential to locate and recover unprotected personal data. Good access controls, policies, and constant vigilance are necessary to ensure that only authorized personnel can access high-risk or high-value data. Organizations can adopt information governance technologies to enforce strict regulations around data privacy and financial information.

References

[1] Felix C Aguboshim, Ifeyinwa N Obiokafor, and Anastasia O Emenike, "Sustainable data governance in the era of global data security challenges in Nigeria: A narrative review," *World J. Adv. Res. Rev.*, vol. 17, no. 2, pp. 378–385, 2023, doi: 10.30574/wjarr.2023.17.2.0154.

[2] R. P. Pratiktio, T. F. Kusumasari, and R. Fauzi, "Design guidelines and process of reference data quality management based on data management body of knowledge," *AIP Conf. Proc.*, vol. 2654, 2023, doi: 10.1063/5.0114293.

[3] W. Febiryani, T. F. Kusumasari, and R. Fauzi, "Analysis and Design of Implementation Guidelines Data Security Management Assessment Techniques Based on DAMA-DMBOKv2," *Proc. - 2021 IEEE 5th Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. Appl. Data Sci. Artif. Intell. Technol. Glob. Challenges Dur. Pandemic Era, ICITISEE 2021*, no. February 2022, pp. 371–375, 2021, doi: 10.1109/ICITISEE53823.2021.9655782.

[4] F. R. Hendrawan, T. F. Kusumasari, and R. Fauzi, "Analysis of Design Implementation Guidelines for Data Governance Management Based on DAMA-DMBOKv2," *2022 7th Int. Conf. Informatics Comput. ICIC 2022*, no. December, 2022, doi: 10.1109/ICIC56845.2022.10007021.

[5] S. Karkošková, "Data Governance Model To Enhance Data Quality In Financial Institutions," *Inf. Syst. Manag.*, vol. 40, no. 1, pp. 90–110, Jan. 2023, doi: 10.1080/10580530.2022.2042628.

[6] W. Amedzro St-Hilaire, "Leading with Digital Technologies Governance in the State-Owned Enterprises," *Int. J. Public Adm.*, vol. 46, no. 2, pp. 107–120, Jan. 2023, doi: 10.1080/01900692.2021.1993898.

[7] K. Dong, R. Lin, X. Yin, and Z. Xie, "How does overconfidence affect information security investment and information security performance?," *Enterp. Inf. Syst.*, vol. 15, no. 4, pp. 474–491, Apr. 2021, doi: 10.1080/17517575.2019.1644672.

[8] The Data Governance Institute, "Data Governance," 2015. https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/.

[9] R. J. Destefano, L. Tao, and K. Gai, "Improving Data Governance in Large Organizations through Ontology and Linked Data," *Proc. - 3rd IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2016 2nd IEEE Int. Conf. Scalable Smart*

Cloud, SSC 2016, pp. 279–284, 2016, doi: 10.1109/CSCloud.2016.47.

[10] C. Indonesia, "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-ramai Bantah," *CNN Indonesia*, 2022. https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah.

[11] Tempo.co, "11 Million Cyber Threats Detected in Indonesia Apart from Bjorka," *Tempo.co*, 2022. https://en.tempo.co/read/1636709/11-million-cyber-threats-detected-in-indonesia-apart-from-bjorka.

[12] C. Indonesia, "13 Juta Data Bocor Bukalapak Dijual di Forum Hacker," *CNN Indonesia*, 2020. https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker.

[13] Liputan 6, "2 Juta Data Nasabah BRI Life Diduga Bocor dan Dijual di Internet," *Liputan 6*, 2020. https://www.liputan6.com/tekno/read/4617605/2-juta-data-nasabah-bri-life-diduga-bocor-dan-dijual-di-internet.

[14] Expert Kaspersky, "Kaspersky Security Bulletin 2020-2021. EU statistics," *Secur. by Kaspersky*, 2021, [Online]. Available: https://securelist.com/kaspersky-security-bulletin-2020-2021-eu-statistics/102335/.

[15] N. Dobberstein, D. Gerdemann, C. Triplett, G. Pereira, G. Hoe, and S. Azhari, "Cybersecurity in ASEAN: An Urgent Call to Action," *ATKearney*, pp. 1–54, 2018, [Online]. Available: https://www.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN—An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34.

[16] B. Engels, "Data Governance as the Enabler of the Data Economy," *Intereconomics*, vol. 54, no. 4, pp. 216–222, 2019, doi: 10.1007/s10272-019-0827-y.

[17] V. Anu, "Information security governance metrics: a survey and taxonomy," *Inf. Secur. J. A Glob. Perspect.*, vol. 31, no. 4, pp. 466–478, Jul. 2022, doi: 10.1080/19393555.2021.1922786.

[18] L. Sun, H. Zhang, and C. Fang, "Data security governance in the era of big data: status, challenges, and prospects," *Data Sci. Manag.*, vol. 2, no. June, pp. 41–44, 2021, doi: 10.1016/j.dsm.2021.06.001.

[19] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services-Use cases, security benefits and challenges," *2018 15th Learn. Technol. Conf. L T 2018*, pp. 112–119, 2018, doi: 10.1109/LT.2018.8368494.

[20] I. Alhassan, D. Sammon, and M. Daly, "Critical success factors for data governance: a telecommunications case study," *J. Decis. Syst.*, vol. 28, no. 1, pp. 41–61, 2019, doi: 10.1080/12460125.2019.1633226.

[21] J. Alghazo, O. K. M. Ouda, and A. El Hassan, "E-waste environmental and information security threat: GCC countries vulnerabilities," *Euro-Mediterranean J. Environ. Integr.*, vol. 3, no. 1, 2018, doi: 10.1007/s41207-018-0050-4.

[22] N. Gupta, S. Blair, and R. Nicholas, "What We See, What We Don't See: Data Governance, Archaeological Spatial Databases and the Rights of Indigenous Peoples in an Age of Big Data," *J. F. Archaeol.*, vol. 45, no. sup1, pp. S39–S50, Feb. 2020, doi: 10.1080/00934690.2020.1713969.

[23] P. Dourish and E. Gómez Cruz, "Datafication and data fiction: Narrating data and narrating with data," *Big Data Soc.*, vol. 5, no. 2, pp. 1–10, 2018, doi: 10.1177/2053951718784083.

[24] P. Brous and M. Janssen, "Trusted decision-making: Data governance for creating trust in data science decision outcomes," *Adm. Sci.*, vol. 10, no. 4, 2020, doi: 10.3390/admsci10040081.

[25] I. Alhassan, D. Sammon, and M. Daly, "Data governance activities: a comparison between scientific and practice-oriented literature," *J. Enterp. Inf. Manag.*, vol. 31, no. 2, pp. 300–316, 2018, doi: 10.1108/JEIM-01-2017-0007.

[26] M. Al-Ruithe, E. Benkhelifa, and K. Hameed, "A systematic literature review of data governance and cloud data governance," *Pers. Ubiquitous Comput.*, vol. 23, no. 5–6, pp. 839–859, 2019, doi: 10.1007/s00779-017-1104-3.
[27] S. AKLEYLEK and C. ATAÇ, "A Survey on Security Threats and Solutions in the Age of IoT," *Avrupa Bilim ve Teknol. Derg.*, vol. 0, no. 15, pp. 36–42, 2019, doi: 10.31590/ejosat.494066.
[28] R. Abraham, J. Schneider, and J. vom Brocke, "Data governance: A conceptual framework, structured review, and research agenda," *Int. J. Inf. Manage.*, vol. 49, pp. 424–438, 2019, doi: https://doi.org/10.1016/j.ijinfomgt.2019.07.008.
[29] V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," *Int. J. Crit. Infrastruct. Prot.*, vol. 39, no. November, p. 100571, 2022, doi: 10.1016/j.ijcip.2022.100571.
[30] R. I. Permana and J. S. Suroso, "Data Governance Maturity Assessment at PT. XYZ. Case Study: Data Management Division," *Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018*, no. March, pp. 15–20, 2018, doi: 10.1109/ICIMTech.2018.8528142.
[31] M. Pelteret and J. Ophoff, "A review of information privacy and its importance to consumers and organizations," *Informing Sci.*, vol. 19, no. 1, pp. 277–301, 2016, doi: 10.28945/3573.
[32] V. W. S. Soemarwi and W. Susanto, "Digital Technology Information in Indonesia: Data Privacy Protection is a Fundamental Right," *Proc. Int. Conf. Econ. Business, Soc. Humanit. (ICEBSH 2021)*, vol. 570, no. Icebsh, pp. 561–566, 2021, doi: 10.2991/assehr.k.210805.088.
[33] United Nations Development Group, "UNDG Guidance Note on Big Data for Achievement of the 2030 Agenda : Data Privacy, Ethics, and Protection," p. 16, 2017, [Online]. Available: https://unsdg.un.org/sites/default/files/UNDG_BigData_final_web.pdf.
[34] DAMA International, *DAMA-DMBOK: Data Management Body of Knowledge (2nd Edition)July 2017*, vol. 44, no. 8. 2017.
[35] H. N. Prasetyo and S. Kridanto, "Perbandingan Framework Tata Kelola Data DGI dan DAMA International," *Pros. Semin. Nas. Apl. Teknol. Inf.*, pp. 27–32, 2013.
[36] F. R. Hendrawan, T. F. Kusumasari, and R. Fauzi, "Analysis of Design Implementation Guidelines for Data Governance Management Based on DAMA-DMBOKv2," *2022 7th Int. Conf. Informatics Comput. ICIC 2022*, 2022, doi: 10.1109/ICIC56845.2022.10007021.
[37] Dama International, *DAMA-DMBOK 2nd edition*, Second Edi. Basking Ridge, NJ 07920 USA: Technics Publications, 2017.
[38] & Mosley, M., Brackett, M., Earley, S. and D. Henderson, *The DAMA Guide to The Data Management Body of Knowledge (DAMA-DMBOK Guide)*, 1st ed. United States of America: Technics Publications, LLC, 2009.
[39] A. A. Afifi and S. V. S. Sastry, "DAMA-DMBOK: Data Management Body of Knowledge," *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2013.
[40] DAMA-DMBOK, *The DAMA Guide to The Data Management Body of Knowledge*. 2009.
[41] DAMA International Technics, *DAMA-DMBOK: Data Management Body of Knowledge: 2nd Edition*. 2017.