International Journal of Emerging Research in Engineering, Science, and Management
Vol. 4, Issue 3, pp.08-14, Jul-Sep 2025.
www.ijeresm.com eISSN – 2583-4894

Integrating COBIT and ISO Frameworks in IT Audits: A Literature Review

[1]Muhammad Fauzan Hanif, [2]Ahmad Rofik Harahap, [3]Ade Fakhrudin, [4]Fadli Fatih Madina, [5]Dimas Febriawan

[1,2,3,4,5]Department of Industrial Technology and Informatics, University of Muhammadiyah Prof. Dr. HAMKA, Jakarta, Indonesia
[1]2203015080@uhamka.ac.id, ORCID: 0009-0004-3684-1407, [2]2203015084@uhamka.ac.id, ORCID: 0009-0003-2549-3024, [3]2203015078@uhamka.ac.id, [4]2203015013@uhamka.ac.id, [5]dimas.febriawan@uhamka.ac.id

Abstract: The accelerated evolution of information technology (IT) has compelled organizations to adopt structured governance frameworks to enhance audit efficacy and ensure robust information security. This study presents a systematic literature review examining the integration of COBIT and ISO/IEC 27001 within IT audit practices. Employing a qualitative descriptive methodology, the review synthesizes insights from seven primary scholarly sources, including case studies from both public and private sectors. The analysis delineates integration patterns, identifies best practices, and explores the synergistic potential of aligning COBIT's strategic governance capabilities with the technical control rigour of ISO/IEC 27001. Findings demonstrate that such integration enhances audit capability maturity, facilitates structured risk mitigation, and fosters alignment between IT functions and organizational objectives. Nonetheless, notable research gaps persist, particularly the scarcity of quantitative assessments, limited cross-sector generalizability, and the absence of longitudinal evaluations of implementation outcomes. Additionally, practical challenges—including integration complexity, inadequate human resource competencies, and the lack of standardized implementation guidelines—impede broader adoption. The study concludes that integrating COBIT and ISO/IEC 27001 constitutes a viable foundation for advancing IT governance and audit maturity. However, further empirical investigation and development of pragmatic toolkits are essential. These insights aim to inform auditors, IT governance professionals, and policy makers in devising adaptive, standard-aligned audit strategies.

Keywords: COBIT, ISO/IEC 27001, IT Audit, Risk Management.

1 INTRODUCTION

The advancement of information technology (IT) has revolutionized how organizations worldwide conduct business operations, deliver public services, and make strategic decisions. Digitalization enables operational efficiency, real-time data access, and cross-sector collaboration. However, this digital transformation also brings significant challenges, including increased risks of data breaches, cyber threats, and the growing complexity of managing information systems. In this context, IT governance (ITG) plays a critical role in ensuring that IT effectively supports organizational goals and delivers value within acceptable risk boundaries [1]. The demand for accountability and effective risk management continues to rise, particularly following the implementation of global regulations such as the Sarbanes-Oxley Act (SOX) in the United States. This regulation requires companies to reevaluate their governance structures to ensure transparency and accountability to shareholders and stakeholders [2]. As a result, organizations are increasingly committed to adopting effective IT governance practices that are integrated with their business strategies. Gartner even reported that ITG has remained one of the top priorities for Chief Information Officers (CIOs) from 2007 to 2009 [3].

Various frameworks have been developed to support the implementation of ITG, such as COBIT 2019, ITIL 4, and ISO/IEC 27001. COBIT serves as a comprehensive guideline for managing IT to achieve business value, ITIL focuses on IT service management, and ISO 27001 emphasizes information security. Several studies have shown that integrating these frameworks can enhance service management capabilities, audit efficiency, and protection of organizational information assets [3][4]. Despite their benefits, the implementation of these frameworks still faces challenges in both public and private institutions. Common issues include suboptimal alignment between organizational goals and framework processes, failure to meet expected process capability levels, and low user satisfaction with IT services [5][4]. Additionally, organizations often struggle to determine the most appropriate integration approach tailored to their specific needs and characteristics [6].

Based on the background and issues identified, this study aims to examine various approaches to integrating the COBIT and ISO frameworks, particularly ISO/IEC 27001, in the context of IT audits through a literature review. The main objective is to identify the best practices, implementation challenges, and the individual contributions of each framework to the effectiveness and efficiency of IT audits. By reviewing scholarly sources and case studies, this research aims to provide a comprehensive understanding of how the integration of COBIT and ISO can strengthen IT governance structures, enhance the reliability of internal controls, and fulfil regulatory and information security requirements.

The expected outcome is to offer both academic and practical references for auditors, IT managers, and policymakers seeking to adopt or develop standardized, complementary audit strategies.

2 Literature Survey

IT governance serves as a strategic mechanism that aligns organizational business goals with the capabilities of information technology. It defines decision-making structures, assigns responsibilities, and enforces oversight to ensure that IT delivers business value while remaining within acceptable levels of risk [7][3]. From an audit standpoint, effective governance supports continuous evaluations of internal control effectiveness, policy compliance, and the mitigation of evolving IT threats. In modern IT auditing, the scope has expanded beyond mere compliance to include strategic alignment, risk management [8], and efficient use of IT resources. As a result, adopting structured frameworks such as COBIT and ISO/IEC 27001 has become increasingly important in achieving measurable and well-governed IT risk management.

COBIT (Control Objectives for Information and Related Technologies), developed by ISACA, provides a governance framework that aligns IT processes with business objectives through structured design factors and a goal cascade approach [1][4]. COBIT 2019, the latest version, categorizes IT governance into five domains: Evaluate, Direct and Monitor (EDM); Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Service and Support (DSS); and Monitor, Evaluate and Assess (MEA). In practical applications, Wulyatiningsih et al. implemented COBIT 2019 in Bank Mandiri Girian Bitung, using 11 design factors to identify key IT processes such as Managed Projects (BAI11), IT Changes (BAI06), and Requirements Definition (BAI02) that directly impact service stability and customer satisfaction [7]. Similarly, Nachrowi et al. (2020) combined COBIT 2019 and ITIL 4 to evaluate digital public service governance using SWOT analysis and e-GovQual to assess user satisfaction in a government setting [1].

On the other hand, ISO/IEC 27001 focuses on operational and technical controls within an Information Security Management System (ISMS), comprising 114 controls across 14 domains, including access control, asset management, and legal compliance. The integration of COBIT and ISO/IEC 27001 provides a complementary approach, with COBIT focusing on strategic and managerial aspects, and ISO/IEC 27001 addressing detailed security controls. Aflakhah and Soewito highlighted how combining the two frameworks enables public organisations to map out comprehensive risk mitigation plans and identify security governance gaps [8]. Nawir et al. demonstrated that aligning COBIT processes with ISO controls yields a standardised, robust system for security audits [4]. These integration practices have been successfully implemented across various sectors. Bank Mandiri Girian Bitung focused on strategic process prioritisation, while a government directorate utilised both frameworks to enhance its cybersecurity readiness. Meanwhile, an education directorate's assessment of e-Government processes revealed low capability levels (0–1), prompting framework-based improvements. Brown & Grant further emphasised the theoretical need for integrated governance frameworks, categorising the evolution of IT governance into structural forms and contingency-based models that bridge formal structures with contextual auditing needs [3].

3 Research Methodology

3.1. Type of Research

This research uses a literature review approach, which aims to identify, analyse, and synthesise the results of previous studies related to the integration of the COBIT and ISO frameworks (especially ISO/IEC 27001) in the context of Information Technology (IT) audits. This approach is used to formulate a conceptual understanding, identify trends, and highlight key findings from the studies that have been conducted.

3.2. Data Sources

The data used in this study comprises scientific articles, accredited journals, and conference proceedings from both national and international sources, all of which are relevant to the theme of COBIT and ISO framework integration. The article selection criteria are as follows:

- Articles published between 2014 and 2024.
- Discuss the COBIT framework (version 5 or 2019) and/or ISO/IEC 27001.
- Focus on the context of IT audit, information security governance, or framework integration.

A total of seven articles were selected and analyzed in this study based on their suitability for the theme.

3.3. Data Collection Techniques

Data was collected through systematic searches using academic search engines such as Google Scholar, IEEE Xplore, Scopus, and Garuda Ristekbrin, using keywords such as:

- COBIT and ISO integration
- IT Governance
- IT Audit Frameworks

Furthermore, articles were selected based on relevance, completeness of content, and contribution to the research topic.

3.4. Data Analysis Techniques

Data analysis was conducted descriptively-qualitatively with the following steps:

- Recording necessary metadata from each article (title, author, year, research context, framework used, methods, and findings).
- Grouping findings based on central themes or issues, such as integration effectiveness, implementation methods, roadmaps, success factors, etc.
- Comparing results between studies to see patterns, differences, and contributions of each article to the understanding of framework integration in IT audit.
- Compiling results in tabular form to make it easier for readers to see comparisons between articles.

4 Results and Discussion

4.1. Results

The objective of this study is to investigate the integration of COBIT and ISO frameworks in IT audits, employing a literature review methodology. A total of seven key articles were chosen due to their direct alignment with the research focus, 'Integrating COBIT and ISO Frameworks in IT Audits: A Literature Review.' The synthesised results are subsequently presented in the table below:

Table 1. Comparison between Selected methods

Author (s)	Research Focus	Framework	Methods	Main Findings
Yasin, Akhmad Arman, Edward and Shalannanda [9]	Designing a roadmap for information security governance at the Indonesian National Police	COBIT 2019 & ISO 27001	DSRM	Integration of 29 COBIT domains with ISO results in a 5-year roadmap towards level 3 capabilities
Aflakhah and Soewito [8]	Information security governance assessment of XYZ Directorate	COBIT 2019 & ISO 27001	Qualitative case study	Average capability 3.07 from 12 domains; mitigation roadmap prepared to close the gap
Gunawan, Hadiprakoso and Kabetta [6]	Comparative study of ITIL+ISO vs COBIT+ISO integration	COBIT 5 & ISO 27001	Literature review	COBIT+ISO integration improves information security at the governance level
Nawir, AP and Wajidi [4]	Information security governance in smart tourism applications	COBIT 2019 & ISO 27001	Qualitative case study	The result is an information security governance policy based on the integration of two frameworks.
Mangalaraj, Singh and Taneja [10]	A systematic review of COBIT literature in IT governance	COBIT	Literature review	COBIT is widely used for audit, security, risk and system development.
Rusman, Nadlifatin and Subriadi [11]	Factors that influence information system audits	COBIT & ITIL	Systematic mapping	Five key factors: design, human resources, operations, risk assessment, audit evidence
Nachrowi, Yani Nurhadryani and Heru Sukoco [1]	Evaluation of IT service governance of the Directorate of Higher Education Institutions	COBIT 2019 & ITIL 4	Evaluasi kualitatif & SWOT	Majority of IT processes are at level 0–1; recommendations for improving HR & service integration

4.2. Discussions

To better understand the integration and implementation of IT governance frameworks, such as COBIT, ITIL, and ISO 27001:2013, in various organisational settings, this section presents a comprehensive discussion of seven selected studies. Each study highlights unique approaches, key findings, and critical insights that contribute to the broader discourse on information system governance and security. The discussions below are structured according to the individual studies that were analysed.

4.2.1. Integrating ISO 27001:2013 and COBIT 2019 for Information Security in Smart Tourism Applications

Nawir, AP and Wajidi conducted an analysis of information security governance for an innovative tourism application managed by PT [4]. YoY Management International is integrating the COBIT 2019 framework with ISO 27001:2013. This study aimed to align the company's strategy with the processes outlined in COBIT 2019, specifically focusing on the APO13 domain, which centres on security management, and then map those processes to the security controls outlined in ISO 27001. The mapping results identified six relevant IT processes, with APO13 selected as the most appropriate to address the company's Information Security Management System (ISMS) needs. The policy recommendations produced include ten key security controls, such as management responsibilities, asset inventory, malware control, and incident response for information security. This study emphasises the significance of business service continuity and availability in the context of the pandemic, as well as the pressing need for user data and privacy protection in application services. The findings offer a valuable contribution to strengthening information security through an integrated framework approach, although the scope is currently limited to a single domain. Future research is suggested to include other domains, such as EDM03, APO12, BAI10, DSS04, and DSS05, for a more comprehensive evaluation [4].

4.2.2. Identifying Critical Factors in Information System Audits Using COBIT and ITIL Frameworks

Rusman, Nadlifatin, and Subriadi conducted a systematic literature review to analyse the factors influencing information systems audits using the COBIT and ITIL frameworks [11]. The study identified five key factors that affect information system audits: design factors, knowledge worker factors, operational factors, risk assessment factors, and evidence collection factors. The study emphasised that improved IT performance drives business growth and competitive advantage, making IT audits increasingly crucial in complex business environments. Furthermore, the study highlighted that the ITIL framework is designed to ensure flexible, coordinated, and integrated systems for effective IT service governance and management. In contrast, the COBIT framework is structured with various components that help customise, maintain, and shape governance systems. Rusman et al. also conducted a systematic mapping study to identify research gaps by mapping the relationships between research topics and the extent to which each has been covered. Visualisation of density mapping showed that "COBIT," "ITIL," "process," and "framework" were heavily researched topics. However, specific studies combining COBIT domains with ITIL practice management remain limited [11].

4.2.3. Comparative Analysis of ITIL and COBIT Integration with ISO/IEC 27001

Gunawan, Hadiprakoso and Kabetta conducted a comparative study on the integration of ITIL and ISO/IEC 27001 versus COBIT and ISO/IEC 27001 [6]. This research used literature studies to compare improvements in information security service credibility, elimination of redundant processes, and enhanced cross-departmental understanding. The results indicated that integrating ITIL and ISO/IEC 27001 enhances the credibility of information security within IT service management, while integrating COBIT and ISO/IEC 27001 improves the credibility of security in IT governance. Both integrations feature several overlapping processes that can be executed simultaneously, facilitating better organisational coordination and understanding. The key difference lies in global recognition, with COBIT being more widely adopted than ITIL. The study also highlighted that COBIT focuses on IT governance in general, while ITIL focuses on service management, and ISO/IEC 27001 targets information security management systems. Nevertheless, integrating COBIT and ISO/IEC 27001 can complement each other to increase organisational benefits, particularly in IT security. This integration can also eliminate redundant processes due to relevant framework mappings [6].

4.2.4. Designing an Information Security Governance Roadmap Using COBIT 2019 and ISO 27001:2013

Yasin, Akhmad Arman, Edward and Shalannanda designed information security governance recommendations and a roadmap using COBIT 2019 and ISO 27001:2013 frameworks, with a case study at Ditreskrimsus Polda XYZ [9]. The study identified that the use of technology in police duties had not yet reached an ideal level of capability in information security management, thus emphasising the need for a structured and practical governance roadmap. The design was carried out based on the six stages of the Design Science Research Methodology (DSRM), including problem identification and motivation, solution objectives definition, design and development, demonstration, evaluation, and communication. By mapping ISO/IEC 27001:2013 to COBIT 2019, 29 core model domains from COBIT 2019 were selected as the basis for designing and assessing the capability levels of information security management at Ditreskrimsus Polda XYZ. The assessment showed that information security governance had not yet reached the target capability level 3.

To achieve this level, the study recommended implementing an organisational structure model, human resources, and relevant policies and procedures in a roadmap from 2021 to 2025. The roadmap includes the gradual fulfilment of 36 human resources and the implementation of 29 relevant policies. While this study contributes to a specific and structured design for information security governance, it does not cover risk management recommendations in line with ISO/IEC 27005:2018, COSO ERM 2017, or other risk management frameworks, presenting an opportunity for future research [9].

4.2.5. Research Trends and Gaps in COBIT Literature: A Comprehensive Review

Mangalaraj, Singh, and Taneja conducted a literature review on IT governance frameworks, particularly COBIT [10]. The study highlighted COBIT's significant role as a comprehensive IT governance framework guiding IT managers in managing and regulating enterprise IT. The primary objective was to compile and analyse existing COBIT research to identify trends and research gaps in the field. Their findings showed that researchers have examined COBIT from various perspectives, with most papers focusing on framework development/comparison or specific areas within COBIT such as security, risk management, system development, effectiveness, and internal control. The study also noted that most papers were published in the accounting domain, despite COBIT's scope having expanded to many areas related to information systems. Mangalaraj et al. identified several future research opportunities in information systems related to COBIT, including IT-business strategic alignment, COBIT adoption, implementation challenges, COBIT effectiveness, and framework customisation. The study emphasised that, although COBIT has existed for nearly two decades, research focus in the information systems domain remains limited, with most studies centred on accounting literature. They concluded that more attention from information systems researchers is urgently needed, given COBIT's critical relevance for IT governance and management in organisations [10].

4.2.6. Evaluating IT Governance and Service Management Using COBIT 2019 and ITIL 4 in Government Institutions

Nachrowi, Yani Nurhadryani and Heru Sukoco evaluated IT governance and service management at the Directorate of Institutional Affairs, Directorate General of Higher Education, using the COBIT 2019 and ITIL 4 frameworks [1]. This evaluation assessed both the IT process capability levels and user satisfaction with the Electronic-Based Government System (SPBE) services. The study revealed that out of eleven assessed processes, three were at level 0 (incomplete), six at level 1 (initial), one at level 2 (managed), and one process reached level 3 (defined). In addition, the user satisfaction assessment using the E-GovQual model showed that out of 31 evaluated attributes, three were in quadrant A (priority for improvement), 13 in quadrant B (maintain performance), 12 in quadrant C (low priority), and 3 in quadrant D (possible overkill). The SWOT analysis generated several strategic recommendations, including enhancing human resource competencies, strengthening risk and information security management, and integrating services with the national higher education database (PDDIKTI). This study emphasises that the integrated application of COBIT 2019 and ITIL 4 can significantly improve the quality of IT governance and public service delivery within government institutions, with notable impacts on efficiency, transparency, and the achievement of strategic organisational goals [5].

4.2.7. Assessing Information Security Governance Using COBIT 2019 and ISO 27001:2013 for Risk Mitigation

Aflakhah and Soewito evaluated information security governance at the Directorate General XYZ by integrating the COBIT 2019 framework with ISO 27001:2013 [8]. The study aimed to design a risk mitigation model based on comprehensive information security governance to address various cyberattacks and identify system vulnerabilities. The research identified 12 key domains within COBIT 2019, including EDM03, APO13, and DSS05, and mapped them to ISO 27001:2013 clauses to develop relevant security policies. Using the Design Science Research Methodology (DSRM) approach, the researchers successfully assessed the organisation’s maturity level, which averaged 3.07 out of a target of 5, indicating a significant gap in information security management. The assessment employed instruments based on the RACI Chart and the KAMI Index version 4.2, producing a detailed recommendation map for each domain. This included improvements in risk management, security process documentation, IT configuration adjustments, and the development of a business continuity plan. The results indicate that information security governance remains suboptimal and requires reinforcement in key areas, including policy documentation, access control, and incident response. This study highlights that the integration of COBIT 2019 and ISO 27001:2013 can serve as a strategic foundation for designing an adaptive, relevant, and needs-based information security roadmap tailored to the complexity of public sector organizations such as the Directorate General XYZ [8][12].

5 Research Gaps and Challenges

Based on the results of the literature review in section 4, there are several research gaps and main challenges in the implementation and development of the integration of the COBIT and ISO frameworks in IT audits.

5.1. Research Gaps

1. Lack of Quantitative Studies and Generalisation of Findings: Most studies employ a case study or qualitative descriptive approach, which makes it challenging to generalise the results to different industry sectors or broader geographic areas.
2. Lack of In-depth Comparative Studies of Framework Integration: Very few works explicitly compare the integration of COBIT+ISO and ITIL+ISO. A systematic comparative study across frameworks can enrich the understanding of the effectiveness of integration in different contexts.
3. Limitations of Implementation Effectiveness Assessment: Many studies produce roadmaps or recommendations but are not accompanied by evaluations of long-term implementation success. No studies have assessed the actual impact of framework integration on audit quality or IT performance on a longitudinal basis.
4. Neglect of Social and Cultural Factors of the Organisation: Most research focuses on technical and process aspects; however, factors such as organisational culture, resistance to change, and HR readiness have not been explicitly studied as determinants of implementation success.

5.2. Challenges

1. Complexity of Synchronising Two Frameworks: Integration between COBIT and ISO 27001 requires a proper mapping of processes, controls, and domains, which can be a significant challenge for organisations that lack IT governance maturity.
2. Resource Requirements and HR Competencies: Integration implementation requires HR professionals who understand both frameworks in depth. Lack of training or limited competencies can hinder the effectiveness of implementation.
3. Dependence on Organisational Context: Integration effectiveness is highly dependent on the type of organisation, its structure, and its specific needs. Not all approaches can be applied uniformly.
4. Lack of Standardised Practical Guidelines: Currently, there are not many guidelines or toolkits available to support the integration process in a practical and scalable way, especially in organisations with limited resources.

6 CONCLUSIONS

Based on the results of the literature review of seven relevant main articles, it can be concluded that the integration between the COBIT framework and ISO 27001 provides a significant contribution to improving the effectiveness of information system audits and IT security governance. This integration helps organisations in developing strategic roadmaps, assessing current capabilities, and designing more structured security policies that comply with international standards. Studies such as those conducted by Yasin et al. and Soewito & Aflakhah show the practical application of framework integration in the context of government institutions, while Gunawan and Nawir et al. illustrate the benefits of integration in increasing the credibility of information security in the public and private sectors. The study by Rusman et al. also highlights the importance of internal factors such as human resources and evidence collection in supporting the success of framework-based IT audits. However, there are research gaps in the form of limited quantitative studies, a lack of practical guidance, and minimal long-term evaluation of the effectiveness of implementing COBIT and ISO integration. Therefore, future research is highly recommended to explore cross-sector approaches, use quantitative methodologies, and develop applicable frameworks that various types of organisations can apply.

FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ETHICS STATEMENT

This study did not involve human or animal subjects and, therefore, did not require ethical approval.

STATEMENT OF CONFLICT OF INTERESTS

The authors declare no conflicts of interest related to this study.

LICENSING

This work is licensed under a Creative Commons Attribution 4.0 International License.

REFERENCES

[1] E. Nachrowi, N. Y. Nurhadryani, and N. H. Sukoco, "Evaluation of Governance and Management of Information Technology Services using COBIT 2019 and ITIL 4," *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, vol. 4, no. 4, pp. 764–774, Aug. 2020, doi: 10.29207/resti.v4i4.2265.

[2] R. Almeida, R. Pereira, and M. M. Da Silva, "IT governance mechanisms patterns," in *Lecture notes in business information processing*, 2013, pp. 156–161. doi: 10.1007/978-3-642-38490-5_13.

[3] Allen E. Brown, Gerald G. Grant, "Framing the Frameworks - A Review of IT Governance Research", *Communications of the Association for Information Systems,* 15, pp. 696–712, 2005. doi: 10.17705/1CAIS.01538.
[4] M. Nawir, I. Ap, and F. Wajidi, "Integration of Framework ISO 27001 and COBIT 2019 in Smart Tourism Information Security Pt. Yoy International Management," *Jurnal Komputer Dan Informatika*, vol. 10, no. 2, pp. 122–128, Sep. 2022, doi: 10.35508/jicon.v10i2.7985.
[5] A. Zein, S. Farizy, E. Suharyanto, C. Tristianto, and F. Marwati, "Information Technology governance between ISO 38500, Risk it and Val it in private university," *Journal of Information System Technology and Engineering*, vol. 2, no. 3, pp. 280–286, Sep. 2024, doi: 10.61487/jiste.v2i3.82.
[6] N. K. Gunawan, R. B. Hadiprakoso, and H. Kabetta, "Comparative Study Between the Integration of ITIL and ISO / IEC 27001 with the Integration of COBIT and ISO / IEC 27001," *IOP Conference Series Materials Science and Engineering*, vol. 852, no. 1, p. 012128, Jul. 2020, doi: 10.1088/1757-899x/852/1/012128.
[7] Toetik Wulyatiningsih, Wilsen Grivin Mokodaser, Joe Yuan Mambu, "Information Technology Governance Analysis Using COBIT 2019 Framework at Bank Mandiri Girian Bitung Branch," *International Journal of Engineering, Science and Information Technology*, vol. 4, no.4, pp. 211–218. 10.52088/ijesty.v4i4.642.
[8] Elok Aflakhah, Benfano Soewito, "Assessing Information Security Using COBIT 2019 and ISO 27001:2013 for Developing a Mitigation Plan," *International Journal of Engineering Trends and Technology,* vol. 71, no. 10, pp. 223-237, 2023. doi: 10.14445/22315381/IJETT-V71I10P221.
[9] M. Yasin, A. Akhmad Arman, I. J. M. Edward and W. Shalannanda, "Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)," *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA*, Bandung, Indonesia, 2020, pp. 1-5, doi: 10.1109/TSSA51342.2020.9310875.
[10] G. Mangalaraj, A. Singh, and A. Taneja, "IT governance frameworks and COBIT - A literature review", *20th Americas Conference on Information Systems, AMCIS 2014*, pp. 1–10, 2014.
[11] A. Rusman, R. Nadlifatin, and A. P. Subriadi, "Information System Audit using COBIT and ITIL Framework: Literature review," *SinkrOn*, vol. 7, no. 3, pp. 799–810, Jul. 2022, doi: 10.33395/sinkron.v7i3.11476.
[12] G. Bongiorno, D. Rizzo, D. *CIOs and the Digital Transformation*, *CIOs and the Digital Transformation*. Springer, 2018. doi: 10.1007/978-3-319-31026-8.